(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－331106
（P2001－331106A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		
Ｇ０６Ｔ　1/00	５００	Ｇ０６Ｔ　1/00	５００Ｂ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	
20/12		20/12		
Ｈ０４Ｌ　9/08		Ｈ０４Ｎ　1/387		

審査請求　未請求　請求項の数20　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願2001－59717(P2001－59717)

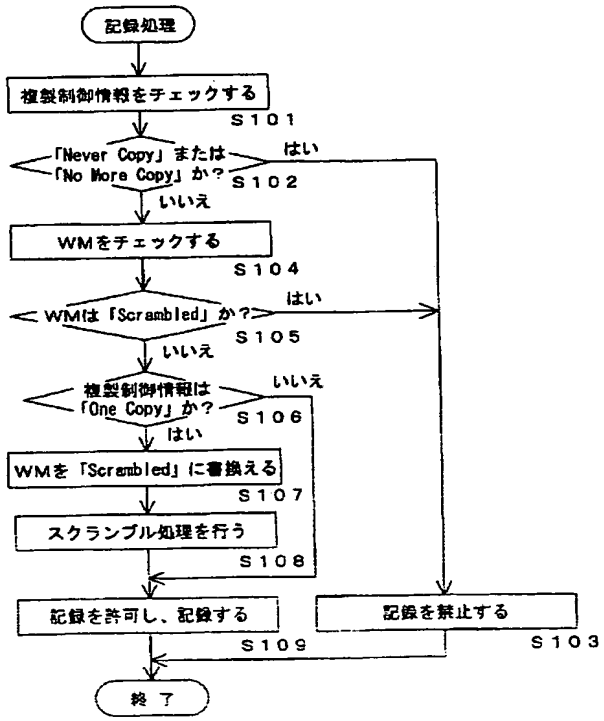
(22)出願日　平成13年３月５日(2001.3.5)

(31)優先権主張番号　特願2000－70020(P2000－70020)
(32)優先日　平成12年３月14日(2000.3.14)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　永井　隆弘
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　石原　秀志
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　福島　能久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100062144
弁理士　青山　葆　（外２名）

(54)【発明の名称】　暗号化情報信号、情報記録媒体、情報信号再生装置、および、情報信号記録装置

(57)【要約】
【課題】　記録媒体の種類にかかわらず、不正に作成された記録媒体からの情報信号の再生を実質的に不能にでき、有効かつ安価に複製の防止ができるようにする。
【解決手段】　複製制御の対象とされる情報信号を暗号化した暗号化情報信号であって、前記情報信号は、前記情報信号が暗号化された状態の信号であることを識別する識別情報が電子透かし情報として重畳された信号である、暗号化情報信号、その信号を記録した情報記録媒体、その信号を再生する情報信号再生装置、および、その信号を記録する情報信号記録装置を提供する。



1

【特許請求の範囲】

【請求項１】　複製制御の対象とされる情報信号を暗号化した暗号化情報信号であって、前記情報信号は、
前記情報信号が暗号化された状態の信号であることを識別する識別情報が電子透かし情報として重畳された信号である、暗号化情報信号。

【請求項２】　前記情報信号は、これ以上の複製禁止、および、絶対複製禁止の少なくとも一方の制限が課された情報信号である、請求項１に記載の暗号化情報信号。

【請求項３】　前記電子透かし情報は、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含む、請求項１に記載の暗号化情報信号。

【請求項４】　請求項１に記載の暗号化情報信号が記録された情報記録媒体。

【請求項５】　暗号化された第１の鍵と、暗号化された第２の鍵とがさらに記録された情報記録媒体であって、
前記第１の鍵は、電子透かし情報が重畳された前記情報信号を暗号化するために用いられた鍵であり、
前記第２の鍵は、前記第１の鍵を暗号化するために用いられた鍵である、請求項４に記載の情報記録媒体。

【請求項６】　請求項４に記載の情報記録媒体から暗号化情報信号を読み出す読み出し部と、
読み出し部が読み出した前記暗号化情報信号が暗号化されている状態であることを判別する暗号化状態判別部と、
前記暗号化情報信号を解読して電子透かし情報が重畳された情報信号を取り出す解読部と、
解読部が解読した前記情報信号から前記電子透かし情報を抽出して、前記識別情報の示す内容を判別する電子透かし情報デコード部と、
暗号化状態判別部により判別された状態と、電子透かし情報デコード部により判別された識別情報の示す状態とを比較し、一致しない場合には前記情報信号の再生を禁止する再生制御部と、
を備えた情報信号再生装置。

【請求項７】　暗号化状態判別部は、解読部が情報信号を取り出した場合には、前記暗号化情報信号は暗号化されている状態であると判別する、請求項６に記載の情報信号再生装置。

【請求項８】　前記電子透かし情報は、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含み、
情報信号再生装置は、前記情報記録媒体の種別を判別する種別判別部をさらに備え、
前記種別情報により表された情報記録媒体の種別と、種別判別部により判別された情報記録媒体の種別とが一致する場合に、再生制御部は前記情報信号の再生を許可する、請求項６に記載の情報信号再生装置。

【請求項９】　前記情報記録媒体には、暗号化された第１の鍵と、暗号化された第２の鍵とがさらに記録されており、前記第１の鍵は、電子透かし情報が重畳された前記情報信号を暗号化するために用いられた鍵であり、前記第２の鍵は、前記第１の鍵を暗号化するために用いられた鍵であり、
解読部は、前記第２の鍵を暗号化するために用いられ、情報信号再生装置に固有に割り当てられた第３の鍵を保持しており、前記第３の鍵で暗号化された第２の鍵を解読して前記第２の鍵を取得し、取得した前記第２の鍵で暗号化された第１の鍵を解読して前記第１の鍵を取得し、取得した前記第１の鍵で前記暗号化情報信号を解読して電子透かし情報が重畳された情報信号を取り出す、請求項６に記載の情報信号再生装置。

【請求項１０】　情報信号再生装置は、
読み出し部、暗号化状態判別部、および、種別判別部を含み、さらに第１の認証部を含むドライブ装置と、
解読部、電子透かし情報デコード部、および、再生制御部を含み、さらに第２の認証部を含むデコード装置と、
ドライブ装置とデコード装置とを接続するインターフェースとから構成されており、
前記第１の認証部と前記第２の認証部とは、前記インターフェースを介して通信して、前記第１の認証部はデコード装置がコンプライアントな装置であるか否かを認証し、前記第２の認証部はドライブ装置がコンプライアントな装置であるか否かを認証し、
前記第１の認証部と前記第２の認証部との間で認証が成立した場合に、再生制御部は前記情報信号の再生を許可する、請求項８に記載の情報信号再生装置。

【請求項１１】　前記情報記録媒体には、前記第１の認証部および前記第２の認証部がそれぞれ認証に用いる、第１の認証鍵および第２の認証鍵がさらに記録されており、
第１の認証部は、ドライブ装置に固有に割り当てられた第１のデバイス鍵を有し、前記第１の認証鍵と、前記第１のデバイス鍵と、種別判別部が判別した前記情報記録媒体の種別とに基づいて第１の媒体認証鍵を生成し、
第２の認証部は、デコード装置に固有に固有に割り当てられた第２のデバイス鍵を有し、前記第２の認証鍵と、前記第２のデバイス鍵とに基づいて、第２の媒体認証鍵を生成し、
前記第１の認証部と前記第２の認証部とは、第１の媒体認証鍵と第２の媒体認証鍵とを比較して認証を行う、請求項１０に記載の情報信号再生装置。

【請求項１２】　第２の認証部は、情報記録媒体ごとに異なる認証手順、および、情報信号転送手順のうちの少なくとも一方を利用して情報記録媒体種別を検出する、請求項１１に記載の情報信号再生装置。

【請求項１３】　複製制御の対象とされる情報信号を情報記録媒体に記録する情報信号記録装置であって、
前記情報信号が暗号化された状態の信号であることを識別する識別情報を、電子透かし情報として情報信号に重

畳する電子透かし情報処理部と、
電子透かし情報処理部により前記電子透かし情報が重畳された情報信号を暗号化して暗号化情報信号を生成する暗号化部と、
暗号化部により生成された暗号化情報信号を、情報記録媒体に書き込む書き込み部とを備えた情報信号記録装置。

【請求項１４】　前記情報記録媒体の種別を判別する種別判別部をさらに備え、
前記電子透かし情報は、種別判別部により判別された、前記暗号化情報信号が記録される情報記録媒体の種別を表す種別情報をさらに含む、請求項１３に記載の情報信号記録装置。

【請求項１５】　情報信号に重畳されている電子透かし情報を抽出して、前記識別情報の示す内容を判別する電子透かし情報デコード部と、
電子透かし情報デコード部により判別された前記識別情報に基づいて、記録を許可する記録制御部とをさらに備えた請求項１４に記載の情報信号記録装置。

【請求項１６】　情報信号記録装置は、
書き込み部、種別判別部を含み、さらに第１の認証部を含むドライブ装置と、
暗号化部、電子透かし情報処理部、電子透かし情報デコード部、および、記録制御部を含み、さらに第２の認証部を含むエンコード装置と、
ドライブ装置とエンコード装置とを接続するインターフェースとから構成されており、
前記第１の認証部と前記第２の認証部とは、前記インターフェースを介して通信して、前記第１の認証部はエンコード装置がコンプライアントな装置であるか否かを認証し、前記第２の認証部はドライブ装置がコンプライアントな装置であるか否かを認証し、
前記第１の認証部と前記第２の認証部との間で認証が成立した場合に、記録制御部は前記情報信号の記録を許可する、請求項１５に記載の情報信号記録装置。

【請求項１７】　前記情報記録媒体には、前記第１の認証部および前記第２の認証部がそれぞれ認証に用いる、第１の認証鍵および第２の認証鍵がさらに記録されており、
第１の認証部は、ドライブ装置に固有に割り当てられた第１のデバイス鍵を有し、前記第１の認証鍵と、前記第１のデバイス鍵と、種別判別部が判別した前記情報記録媒体の種別とに基づいて第１の媒体認証鍵を生成し、
第２の認証部は、エンコード装置に固有に固有に割り当てられた第２のデバイス鍵を有し、前記第２の認証鍵と、前記第２のデバイス鍵とに基づいて、第２の媒体認証鍵を生成し、
前記第１の認証部と前記第２の認証部とは、第１の媒体認証鍵と第２の媒体認証鍵とを比較して認証を行う、請求項１６に記載の情報信号記録装置。

【請求項１８】　第２の認証部は、情報記録媒体ごとに異なる認証手順、および、情報信号転送手順のうちの少なくとも一方を利用して情報記録媒体種別を検出する、請求項１７に記載の情報信号記録装置。

【請求項１９】　前記情報記録媒体には、情報信号再生装置に固有に割り当てられた第３の鍵で暗号化された第２の鍵が記録されており、
暗号化部は、
暗号化部の内部で発生させた乱数、前記情報記録媒体に記録された第１の鍵情報、および、電波に重畳された第１の鍵情報のいずれかに基づいて前記第１の鍵を取得して、前記電子透かし情報が重畳された情報信号を第１の鍵で暗号化し、
前記第１の鍵を第２の鍵で暗号化し、
第３の鍵と、情報記録媒体に記録された暗号化された第２の鍵とに基づいて第２の鍵を取得する、請求項１３に記載の情報信号再生装置。

【請求項２０】　書き込み部は、第２の鍵で暗号化された第１の鍵をさらに情報記録媒体に書き込む、請求項１９に記載の情報信号記録装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された著作物、例えば映像、音楽等の情報信号を情報記録媒体に記録する際の不正な複製を制限する技術、および、不正に複製された情報記録媒体からの再生を制限する技術に関する。

【０００２】

【従来の技術】近年、デジタルコンテンツの普及に伴い、デジタルコンテンツの不正な複製による著作権侵害が大きな問題となっている。不正な複製を防止するために、デジタルコンテンツに複製制御のための情報（複製制御情報）を付加したり、または、暗号化技術を用いて情報信号を暗号化し、正式にライセンスを受けた機器以外の機器には復号化（解読）できないようにする技術が考えられている。また、情報信号に対して、複製制御情報をさらに電子透かし情報としても埋め込む技術も存在する。電子透かし情報は雑音として情報信号に重畳され、容易に書き換えられないので、複製制御情報が不正に書き換えられた場合でも再生制御および記録制御を行うことができる。

【０００３】複製制御のために情報信号に付加される情報は、“複製可能（Ｃｏｐｙ　Ｆｒｅｅ）”、“１回複製可能（Ｏｎｅ　Ｃｏｐｙ）”、“これ以上複製禁止（ＮｏＭｏｒｅ　Ｃｏｐｙ）”、“絶対複製禁止（Ｎｅｖｅｒ　Ｃｏｐｙ）”の４状態がある。この４状態によって、情報信号の複製世代や複製制限状態を表現できる。

【０００４】複製の制限は、以下のようにして行われる。すなわち記録装置が画像、音声等の情報信号に含ま

れる複製制御情報をチェックし、複製制御情報が“これ以上複製禁止”や“絶対複製禁止”を表す場合は記録を制限する。これにより、複製世代制限が実現される。しかしながら、複製制御情報をチェックしない記録装置は“これ以上複製禁止”の状態にある情報信号でも記録媒体に記録することができ、さらにこの記録媒体は、複製制御情報を含む元の情報信号と同じ情報信号がそのまま複製された記録媒体である。これでは著作権が保護できない。

【０００５】この問題を解決するための技術として、特開平１１－３５３７９６号公報には、情報信号にさらに電子透かし情報を重畳し、情報信号の再生時に電子透かし情報が示す状態を書き換えることにより、不正に記録された記録媒体からの再生を実質的に不能とする技術が記載されている。

【０００６】より具体的に説明する。この説明中、電子透かし情報の解読処理または書き込み処理に対応することを「コンプライアント」、対応しないことを「ノンコンプライアント」という。図１６は、従来の複製制御の原理を示す図である。ＤＶＤ－ＲＡＭ等のＲＡＭディスク１３００には、“これ以上の複製禁止”を示す複製制御情報（ＣＧＭＳ[１１]）と、同様に“これ以上の複製禁止”を示す電子透かし情報（WM [No More Copy]）とが重畳された情報信号が記録されている。この情報信号の再生に際し、コンプライアント再生装置１３０１は、電子透かし情報を“No More Copy”（これ以上の複製禁止）から、“Never Copy”（絶対複製禁止）に書き換え、情報信号に重畳し直した上で情報信号を再生出力信号として送出する。ＤＶＤ－ＲＡＭでは通常、複製を禁止する場合には“No More Copy”が利用され、“Never Copy”は利用されない。したがって、情報信号に重畳されている電子透かし情報が“Never Copy”であることを検出すると、コンプライアント記録装置１３０２はその情報信号を記録しない。これにより複製を制御できる。

【０００７】一方、ノンコンプライアント記録装置１３０３は、電子透かし情報の内容にかかわらず記録制限なく情報信号を別のＲＡＭディスク１３０４へ記録する。しかしながら、不正に記録されたＲＡＭディスク１３０４の電子透かし情報は“Never Copy”である。したがって、コンプライアント再生装置１３０５は、その電子透かし情報を読み取ることでそのＲＡＭディスク１３０４を不正な複製が行われた記録媒体であると判定し、再生を実質的に不能とする。

【０００８】

【発明が解決しようとする課題】上述のように従来のコンプライアント再生装置１３０１は，複製を制御するために、電子透かし情報の内容を“No More Copy”（これ以上の複製禁止）から、“Never Copy”（絶対複製禁止）に書き換える。このため、再生装置は電子透かし情報の書き換え手段を備えることが不可欠であり、再生装置のコストアップにつながる。

【０００９】また上述の技術は、ＤＶＤ－ＲＯＭには適用できない。ＤＶＤ－ＲＯＭでは、不正か否かを判定するための電子透かし情報“Never Copy”が、通常の使用においてディスクに書き込まれるからである。

【００１０】以上の点に鑑み、本発明の目的は、記録媒体の種類にかかわらず、不正に作成された記録媒体からの情報信号の再生を実質的に不能にすることにより、有効かつ安価に複製の防止ができるようにすることである。

【００１１】

【課題を解決するための手段】上記課題を解決するために、本発明による複製世代管理は、複製制御が必要な情報信号を記録する情報記録媒体において、少なくとも、これ以上の複製禁止、絶対複製禁止の状態の情報信号である前記情報信号には情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号であることを特徴とする。

【００１２】本発明の情報記録再生装置は、これ以上の複製禁止、あるいは、絶対複製禁止の状態である前記情報信号には、情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として重畳され、前記電子透かし情報が重畳された情報信号にスクランブルを施した情報信号として記録された情報記録媒体を読み出す情報再生装置であって、情報記録媒体から情報を読み出す情報読み出し手段と、前記情報信号に対して施されたスクランブルをデスクランブルするデスクランブル手段と、デスクランブルされた情報信号に電子透かし情報として重畳されているスクランブル情報を検出する電子透かし情報検出手段と、前記電子透かし情報とデスクランブル手段のデスクランブル動作を調べ、少なくとも、電子透かし情報のスクランブル情報がスクランブル状態にあり、デスクランブル手段が動作していない場合に、前記情報信号の正常な再生を禁止する再生制御手段とを備える。

【００１３】本発明の情報記録装置は、１回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置であって、前記複製制御情報を検出する手段と、検出した複製制御情報が１回複製可能である場合に、情報記録媒体にスクランブル状態で記録されることを示すスクランブル情報が電子透かし情報として前記情報信号に重畳する電子透かし情報書換手段と、前記電子透かし情報を重畳した情報信号にスクランブルを施すスクランブル手段と、前記スクランブルした情報信号を情報記録媒体に書き込む情報書き込み手段を備える。

【００１４】本発明の情報信号記録装置は、１回複製可能、これ以上の複製禁止、あるいは、絶対複製禁止の状態の複製制御情報を有する前記情報信号を情報記録媒体に書き込む情報記録装置において、前記複製制御情報を検出する複製制御情報検出手段と、前記情報信号に重畳されている電子透かし情報を検出する電子透かし情報検出手段と、前記電子透かし情報として情報信号がスクランブル状態で記録されていることを示すスクランブル情報が検出された場合に、記録を禁止する記録制御手段とを備える。

【００１５】

【発明の実施の形態】以下、添付の図面を参照して、本発明による暗号化情報信号、情報記録媒体、情報信号再生装置、および、情報信号記録装置を説明する。実施の形態では、情報記録媒体はＤＶＤ－ＲＡＭ（ＲＯＭ）に代表される光ディスクであり、この光ディスクに情報信号が記録される。また複製制御の対象は、画像、音声等を表す情報信号、すなわち画像音声情報である。

【００１６】以下の説明では、記録型のＤＶＤをＲＡＭディスク、再生専用のＤＶＤをＲＯＭディスクと称する。また、後述の複製世代制限処理に対応する記録装置および再生装置をコンプライアントの装置と呼び、複製世代制限処理に対応していない装置をノンコンプライアントの装置と呼ぶ。

【００１７】（実施の形態１）図１は、本実施の形態による複製世代管理方法を説明するための概略図である。本実施の形態では、ＲＯＭディスク１００には映像や音声などの情報信号が記録されている。ただし、ＲＯＭディスクに代えてＲＡＭディスクを利用してもよい。

【００１８】まず、本実施の形態における情報信号を説明する。情報信号には、映像や音声などを表す信号の他に、雑音の形で電子透かし情報WM（digital WaterMark）が埋め込まれている。電子透かし情報の特徴は、主に、著作物（映像や音声）の改変や圧縮、伸張処理を行っても電子透かし情報が消えないこと、人間の目や耳では感知しにくいレベルで電子透かし情報が埋め込まれること、および、電子透かし情報を埋め込んでもオリジナルの著作物の品質が保持されることである。この特徴により、不正な書き換えを防止し、再生制御および記録制御を行うことができる。

【００１９】情報信号にはさらに、複製制御情報（図示せず）も記録されている。複製制御情報は、コピー可能か否かを表現できる情報である。例えば、２ビットの情報を用いるＣＧＭＳ（Copy Generation Management System）である。ＣＧＭＳによれば、“００”は「複製フリー」、“０１”は「１回複製可能」、“１０”は「絶対複製禁止」、そして“１１”は「これ以上の複製禁止」を表す。

【００２０】情報信号を複製制御の対象とする場合、例えば情報信号の複製を全く禁止する場合には、正規にライセンスを受けた装置でなければ情報信号を再生できないようにするために、本発明では情報信号をスクランブル（暗号化）して記録する。本発明の特徴的な処理は、情報信号がスクランブルされた情報であることを示すスクランブル情報“Ｓｃｒａｍｂｌｅｄ”を、電子透かし情報WMとして情報信号に重畳することである。したがってスクランブル情報は、情報信号が暗号化されているか否かの状態を識別するために用いられる暗号状態の識別情報ということができる。電子透かし情報を用いた複製制御の詳細な説明は後述する。上述の電子透かし情報の特徴によれば、スクランブル情報“Ｓｃｒａｍｂｌｅｄ”は信号情報の改変、圧縮または伸張処理にかかわらず消えることはないので、検出することができる。スクランブル処理は、電子透かし情報が重畳された情報信号に対して、特定のスクランブル方式（暗号方式）にしたがって行われる。

【００２１】一方、情報信号を複製制御の対象としない場合、例えば、情報信号の自由な複製を許す場合には、情報信号はスクランブルされない。この場合には、信号情報には電子透かし情報が重畳されても、されなくてもよい。電子透かし情報が重畳される場合には、電子透かし情報は、信号情報がスクランブルされていないことを示すスクランブル情報“Ｎｏｎ－Ｓｃｒａｍｂｌｅｄ”となる。記録装置（図示せず）は、スクランブルされていない情報信号をそのまま、または電子透かし情報を重畳した情報信号をディスクに記録し、ＲＯＭディスク１００を製造する。

【００２２】本発明の複製世代管理方法を説明するに先だって、まずＲＯＭディスク１００を製造する際のスクランブル処理の手順を説明する。以下説明するスクランブル処理は、ＲＯＭディスク１００の製造業者がオーサリングシステムおよびディスクカッティングシステムを利用して行う。スクランブル処理の例は、ＤＶＤ－ＲＯＭの著作権保護システムＣＳＳ（Content Scramble System）である。映像、音声等を含む情報信号は、３種類の暗号鍵を階層的に用いて暗号化される。３種類の暗号鍵とは、タイトル鍵、ディスク鍵、および、マスター鍵である。以下、著作権保護システムＣＳＳのコンテンツ暗号化手順に沿って説明する。本明細書では、「スクランブル」という語は「暗号化」を意味する。スクランブルのための暗号方式は、１つの鍵を用いて暗号化を行うアルゴリズムであればよい。したがって、周知のアルゴリズムが利用可能である。アルゴリズムの説明は省略する。なお、このアルゴリズムはセキュリティの観点から非公開とされることが多い。一方、スクランブルされた情報をスクランブルされていない情報に戻すことを「デスクランブル」という。これは、「解読」または「復号化」という語と同義である。

【００２３】スクランブル処理の手順は以下のとおりである。まず、情報信号がＭＰＥＧ圧縮され、その後、タ

イトル鍵を用いてスクランブルされる。タイトル鍵は、著作権者、例えば映画のディレクタがディスクに格納されるタイトル毎、すなわち情報信号の単位毎に自由に選んだ鍵である。スクランブルされた信号情報は、ディスクのデータ記録領域に格納される。

【００２４】次に、タイトル鍵は、ディスク鍵を用いて暗号化される。ディスク鍵とは、著作権管理者、例えば映画会社がディスク毎に自由に選ぶことができる鍵である。ディスクが１つ以上の暗号化タイトルを含む場合、著作権管理者は自由にディスク鍵を決定できる。暗号化されたタイトル鍵は、ユーザがアクセスできない、ディスクのセクターヘッダ領域に格納される。

【００２５】最後に、ディスク鍵はマスター鍵を用いて暗号化され、暗号化されたディスク鍵セットに変換される。マスター鍵とは、スクランブルされた情報信号を復号化するデスクランブル装置のメーカ毎に割り当てられた鍵であり、メーカ毎に異なる。「暗号化されたディスク鍵セット」とは、暗号化されたディスク鍵が１または複数存在することを意味する。これはライセンスを受けたメーカの数だけマスター鍵が存在するので、その数と同じ数の１以上のディスク鍵が生成されるからである。暗号化されたディスク鍵セットは、ユーザがアクセスできない、ディスクのリードイン領域に格納される。

【００２６】以上の処理により、ＲＯＭディスク１００には、スクランブルされた信号情報、暗号化されたタイトル鍵、および、暗号化されたディスク鍵セットが格納されていることになる。

【００２７】複製制御の対象となるＲＯＭディスク１００の情報信号を再生するためには、デスクランブル処理を行う必要がある。デスクランブル処理を行うためには、上述の所定の暗号方式に対するライセンスを受け、復号鍵（マスター鍵）や復号アルゴリズムに関する情報を取得しなければならない。図１に示すような、復号機能を実装したコンプライアント再生装置１０１では、ＲＯＭディスク１００からスクランブルが施されている情報信号を読み出し、デスクランブルを行い、ＭＰＥＧデコード可能な情報信号を得ることができる。

【００２８】以下では、ＤＶＤプレーヤ等の再生機器が行うデスクランブル処理を説明し、次にＤＶＤ－ＲＡＭドライブ等の記録装置が行うスクランブル処理を説明する。図２は、スクランブルされた信号情報の読み出しまたは書き込みを行う際のデータの流れを示す図である。

【００２９】図２の（ａ）は、ディスク２１０に記録された、スクランブルされた情報信号をデスクランブル処理する概念図を示す。ディスク２１０は、ＲＯＭディスク１００（図１）に相当するディスクであり、スクランブルされた情報信号２１２と、暗号化されたタイトル鍵２１４と、暗号化されたディスク鍵セット２１６とが記録されている。ここでは、スクランブルされた情報信号２１２はＭＰＥＧ圧縮された映像音声情報とする。再生機器のデスクランブル部２２０は、情報信号をデスクランブルし、ＭＰＥＧデコードする装置である。デスクランブル部２２０は、ディスク鍵復号化部２２２と、タイトル鍵復号化部２２４と、情報信号復号化部２２６と、ＭＰＥＧデコーダ２２８とを含む。

【００３０】デスクランブル部２２０は、暗号化されたディスク鍵セット２１６、暗号化されたタイトル鍵、および、スクランブルされた情報信号をディスク２１０から読み出す。ディスク鍵復号化部２２２はまず、内部記憶領域（図示せず）に保持した、または再生機器の他の構成要素を介して与えられたマスター鍵を用いて、読み出したディスク鍵セット２１６から自己のディスク鍵を復号化する。次にタイトル鍵復号化部２２４は、復号化したディスク鍵を用いて暗号化されたタイトル鍵２１４を復号化する。そして情報信号復号化部２２６は、復号化したタイトル鍵を用いてスクランブルされた情報信号２１２を復号化する。このようにしてデスクランブル処理が行われる。デスクランブルされた情報信号はＭＰＥＧ圧縮処理されたデータであるので、本実施の形態ではＭＰＥＧデコーダ２２８がデコード処理を行って、映像音声情報を出力する。以上、デスクランブル部２２０の処理を説明した。

【００３１】図２の（ｂ）は、ディスク２３０に記録するために、情報信号をスクランブル処理する概念図を示す。この処理は、例えば「１回複製可能」とされた情報信号を記録する際の処理である。書き込みに用いられるディスク２３０は、製造業者からの出荷時に予め暗号化されたディスク鍵セット２３６が記録されている。

【００３２】まずスクランブル部２４０のＭＰＥＧエンコーダ２４８は、入力された情報信号をＭＰＥＧ圧縮処理し、生成したＭＰＥＧデータを情報信号暗号化部２４６に送る。次に、情報信号暗号化部２４６は、タイトル鍵を用いてＭＰＥＧデータをスクランブル処理する。タイトル鍵は乱数発生器２５０で生成された乱数である。一方タイトル鍵暗号化部２４４は、ディスク鍵を用いてタイトル鍵を暗号化する。暗号化されたタイトル鍵２３４はディスク２３０に記録される。ここで、ディスク鍵は、スクランブル部２４０が保持するマスター鍵を用いて、ディスク２３０に記録された暗号化されたディスク鍵セット２３６から、その記録装置のメーカに対応するディスク鍵を復号化することにより得られる。

【００３３】なお一度タイトル鍵を生成し、暗号化されたタイトル鍵２３４としてディスク２３０に記録すると、その後に情報信号をスクランブル処理して記録する際には記録された暗号化されたタイトル鍵２３４が用いられる。すなわち、スクランブル部２４０はディスクの暗号化されたタイトル鍵２３４を読み出してディスク鍵で復号化し、タイトル鍵を用いて情報信号をスクランブルする。

【００３４】以上のように、スクランブル部２４０は、

２通りの経路でタイトル鍵を取得することができる。すなわち、乱数発生器２５０で発生された乱数をタイトル鍵として取得する場合と、ディスク２３０に記録された暗号化されたタイトル鍵２３４を復号化してタイトル鍵として取得する場合の２つの場合である。将来、番組配信が増加すると、放送業者（コンテンツ製作者）の側でタイトル鍵を生成し、そのタイトル鍵でスクランブルされた情報信号が、デジタル放送として、電波で配信されると考えられる。この場合には、ディスクには、放送業者から取得したタイトル鍵とスクランブルされた情報信号を記録することになる。

【００３５】以上のようにして、情報信号のスクランブル処理およびデスクランブル処理を行う。

【００３６】次に再び図１を参照して、本発明による複製世代管理の原理を説明する。本実施の形態では、信号情報を複製制御の対象とする場合には、その信号情報にはスクランブル情報“Ｓｃｒａｍｂｌｅｄ”が電子透かし情報として重畳されている。ＲＯＭディスク１００には、スクランブル情報“Ｓｃｒａｍｂｌｅｄ”が重畳された信号情報がスクランブルされて記録されているとする。

【００３７】本発明による複製世代管理の主たる特徴は、ディスク上の信号情報のスクランブル状態（すなわちスクランブルされているか否か）と、スクランブル情報の状態（すなわちスクランブル情報が“Ｓｃｒａｍｂｌｅｄ”となっているか否か）とを比較し、比較結果に応じて再生または記録を行うか、それらを制限するかを決定することである。信号情報がスクランブルされているか否かは、信号情報や、関連する付属ファイルの情報の中に所定のフラグが立っているか否か、またはデスクランブル部が正常に動作したか否かで判断する。以下、具体的に説明すると、まず再生装置１０１は、まずＲＯＭディスク１００からスクランブルされた信号情報を読み出して、デスクランブルを行う。そして再生装置１０１はデスクランブルされた信号情報からスクランブル情報を検出し、スクランブル状態が一致するか否かの比較を行う。ここでは、信号情報がスクランブルされている状態であったこと、および、スクランブル情報が“Ｓｃｒａｍｂｌｅｄ”であることから、スクランブル状態は一致すると判断できる。これによりコンプライアント再生装置１０１はデスクランブルした情報信号の出力を行う。このとき留意すべきは、出力される情報信号にはスクランブル情報“Ｓｃｒａｍｂｌｅｄ”が重畳されていることである。電子透かし情報としてのスクランブル情報は、コンプライアント再生装置１０１のデスクランブル処理によっては消えることはないからである。

【００３８】続いて、再生装置から出力された情報信号を記録媒体に不正に記録しようとした場合の、記録が制限される原理を説明する。コンプライアント記録装置１０２は、コンプライアント再生装置１０１からデスクランブルされた情報信号を受け取る。コンプライアント記録装置１０２は、受け取った信号情報がデスクランブル状態であること、および、重畳されたスクランブル情報が“Ｓｃｒａｍｂｌｅｄ”であることを認識する。その結果、出力情報信号の状態とスクランブル情報の示す状態とが不一致なので、コンプライアント記録装置１０２はＲＡＭディスク等の記録媒体への記録を行わない。これによりコンプライアント記録装置１０２では、信号情報の記録を制限できる。

【００３９】一方、情報信号にスクランブルが施されていなかった場合も、同様に、スクランブル状態を比較すればよい。電子透かし情報が検出されない場合、あるいは電子透かし情報“Ｎｏｎ－Ｓｃｒａｍｂｌｅｄ”が検出された場合には情報信号の出力を行う。このように出力された信号は、自由に複製が可能であり、コンプライアント記録装置１０２ではＲＡＭディスクへの情報信号の複製が許可される。

【００４０】次に、情報信号がＲＡＭディスクに不正に複製された場合に、再生が制限される原理を説明する。ノンコンプライアント記録装置１０３は、コンプライアント再生装置１０１が出力したデスクランブルされた情報信号を受け取る。この情報信号はスクランブル情報”Ｓｃｒａｍｂｌｅｄ”を有するので複製制御対象であるが、ノンコンプライアント記録装置１０３は電子透かし情報を検出することなく、情報信号をＲＡＭディスク１０４へ複製する。その後、コンプライアント再生装置１０５でこのようなＲＡＭディスク１０４を再生しようとするとき、コンプライアント再生装置１０５は、スクランブル状態の比較を行う。この場合には、情報信号はデスクランブルされた状態で記録されている一方、情報信号にはスクランブルされていることを示すスクランブル情報”Ｓｃｒａｍｂｌｅｄ”が重畳されている。よってコンプライアント再生装置１０５は、比較結果が不一致となることからそのＲＡＭディスク１０４の情報信号は不正に複製された情報信号であると判断する。これによりコンプライアント再生装置１０５は、情報信号の再生を禁止する。

【００４１】なお再生の制限は、記録の対象がＲＡＭディスク１０４でない場合でも行われる。例えば、記録の対象が、書き込み可能であるが一旦書き込んだ後は読み出し専用のディスクとなるＤＶＤ－Ｒでもよい。

【００４２】より確実に不正な記録および再生を禁止するために、スクランブルの際に用いられる暗号化アルゴリズムを記録媒体の種別に応じて相違させる手法もあわせて用いられている。例えば、ＤＶＤ－ＲＯＭ用の暗号化アルゴリズムとＤＶＤ－ＲＡＭ用の暗号化アルゴリズムとを異ならせることにより、ＤＶＤ－ＲＯＭ用のアルゴリズムでスクランブルした情報信号をＤＶＤ－ＲＯＭからＤＶＤ－ＲＡＭに不正に複製したとしても、ＤＶＤ－ＲＡＭからの再生を禁止できる。この動作を実現する

ためには、例えば、記録媒体の種別と、各種別に用いられる暗号化アルゴリズムとを対応付けるテーブルを設ける等すればよい。デスクランブル回路が、記録媒体の種別に対応する復号化アルゴリズムでデスクランブルできなかった場合には、不正に複製された記録媒体からの信号情報の再生を禁止できる。記録媒体の種別を表す種別情報は、スクランブル情報とともに電子透かし情報として情報信号に重畳されてもよい。種別情報は、記録される記録媒体の種別を表すことになる。したがって、ＤＶＤ－Ｒに記録する場合と、ＤＶＤ－ＲＡＭに記録する場合とも区別できる。

【００４３】以上のように、本発明では、スクランブル（暗号化）された情報信号には、その情報信号が暗号化されていることを示す暗号化情報（スクランブル情報“Ｓｃｒａｍｂｌｅｄ”）を電子透かし情報として重畳させる。信号情報は復号化された場合でも、電子透かし情報は改変されることなくそのままの内容で残る。信号情報が復号化状態（非暗号化状態）を示し、電子透かし情報は暗号化状態を示すので、その不一致を検出することにより、コンプライアント記録装置および再生装置のいずれにおいても、他の記録媒体への不正な記録または不正な記録媒体からの再生を禁止できる。よって、コンプライアント再生装置に電子透かし情報の書換手段を実装しなくても、ノンコンプライアント記録装置１０３によって行われた不正な複製ディスクをコンプライアント再生装置で再生禁止にできる。

【００４４】なお、本実施の形態では、電子透かし情報として情報信号に施されているスクランブル情報（“Ｓｃｒａｍｂｌｅｄ”、“Ｎｏｎ－Ｓｃｒａｍｂｌｅｄ”）を情報信号に重畳したが、情報信号のスクランブルの状態を示すものであれば他の情報を用いてよい。例えば、ＲＯＭディスクにおいて、複製制御情報である“絶対複製禁止”である情報信号に対して情報信号をスクランブルして記録する場合、この複製制御情報を電子透かし情報として情報信号に重畳しても同様の効果が得ることができる。

【００４５】［記録装置］次に図３を参照して、コンプライアント記録装置１０２の構成を説明する。図３は、コンプライアント記録装置１０２の構成を示す。コンプライアント記録装置１０２は、デジタル入力端子３０１とアナログ入力端子３０２とを備える。各々は、暗号鍵情報等のデジタル信号と、映像音声情報等のアナログ信号とを接続された機器から受信する。暗号解読部３０３は、デジタル入力端子に接続される機器から送られてくる暗号鍵情報に基づいて暗号化されたデータを復号化し、圧縮ビデオデータを復元する。この際、入力された情報信号がコピー可能であるかどうかを示す複製制御情報を検出する。複製制御情報も、情報信号に重畳された情報である。

【００４６】また、アナログ入力端子３０２を通じて入力された映像情報は、アナログ入力端子３０２を通じてエンコード部３０４に供給され、ＭＰＥＧ圧縮される。その結果、圧縮映像データが生成される。この際、入力された情報信号が複製可能であるかどうかを示す複製制御情報を検出する。

【００４７】セレクタ３０５はユーザの入力選択に応じたセレクタ制御信号により、暗号解読部３０３からのデータと、エンコード部３０４からのデータとのいずれかを選択して出力する。

【００４８】このセレクタ３０５から出力されるデータは、ＷＭ書換部３０６を介して記録制御部３０８に供給される。ＷＭ書換部３０６は、電子透かし情報として情報信号にスクランブル情報“Ｓｃｒａｍｂｌｅｄ（ＲＡＭ）”を重畳するための処理を行う。ただし、この処理は後に説明する記録媒体の種別の判別を行った上で行う必要がある。ＷＭ書換部３０６の処理は、例えば、擬似雑音符号系列の符号を用いてスクランブル情報をスペクトラム拡散し、スペクトラム拡散したスクランブル情報を出力する。これは周知の技術であるから、詳細な説明は省略する。セレクタ３０５から出力されるデータは、ＷＭデコード部３０７にも供給される。ＷＭデコード部３０７は、電子透かし情報として情報信号に重畳されているスクランブル情報の抽出、記述内容の判別を行い、判別出力をコントロール部３０９に供給する。

【００４９】コントロール部３０９は入力情報から検出された複製制御情報および電子透かし情報の判別出力に基づいて、入力情報の記録（複製）が可能であるか否かの判別を行い、記録（複製）可能であると判別した場合は、さらに、複製制御のために電子透かし情報の書換えが必要であるか否かを判別する。そして記録禁止と判別したときには、コントロール部３０９は、記録制御部３０８が記録を実行しないよう制御する。また、記録可能、または、１回複製可能と判別したときには、コントロール部３０９は記録制御部３０８に記録を実行させる。このとき、記録装置１０２は、読み出し部３１３を介してディスクの種別（ＲＡＭディスク、１回のみ書き込み可能なディスク等のタイプ）に関する情報を読み出し、ディスク種別判別部３１４でそのディスクの種別を判別する。その結果、先に説明したようなスクランブル情報の内容が決定され、ＷＭ書き換え部３０６において情報信号に重畳すべきスクランブル情報が生成され、記録制御部３０８において情報信号に重畳される。情報信号は、スクランブル部３１０によりそのディスクの種別に応じた特定のスクランブルを施され、書き込み部３１１を介してＲＡＭディスク３１２に記録される。

【００５０】次に図４を参照して、コンプライアント記録装置１０２が暗号解読を終了した後の処理を説明する。図４は、記録装置１０２の記録処理フローを示すフローチャートである。

【００５１】まず、情報信号が入力された時に検出した

複製制御情報をチェックする（ステップＳ１０１）。そして、複製制御情報が“Never Copy”（絶対複製禁止）または、“No More Copy”（これ以上複製禁止）であるか否かを判別する（ステップＳ１０２）。いずれかに該当する場合には、記録を禁止し、記録処理を中止する（ステップＳ１０３）。なお“Never Copy”（絶対複製禁止）とは、情報信号の複製が全く禁止されるという制限が課されることを表す。一方、“No More Copy”（これ以上複製禁止）は、１回だけ複製可能の音楽データや画像データが複製された場合に、これ以上の情報信号の複製が禁止されるという制限が課されることを表す。いずれにも該当しない場合（“Never Copy”または“No More Copy”でない場合）には、入力信号に重畳されている電子透かし情報（ＷＭ）の判定出力をチェックし（ステップＳ１０４）、電子透かし情報（ＷＭ）が“Ｓｃｒａｍｂｌｅｄ”の状態であるかどうかを判別する（ステップＳ１０５）。“Ｓｃｒａｍｂｌｅｄ”の状態であれば、記録しようとしている情報信号は元々スクランブルされていた情報であることから、この情報信号が複製制御情報を不正に改竄して入力された情報であると判断し、記録処理を中止する（ステップＳ１０３）。“Ｓｃｒａｍｂｌｅｄ”の状態でなければ、記録可能な情報であると判断できる。

【００５２】記録可能な情報であると判断すると、次にその情報信号をスクランブルする必要があるか否かを判断するために、複製制御情報が“１回複製可能（Ｏｎｅ　Ｃｏｐｙ）”の状態にある情報信号か否かを判別する（ステップＳ１０６）。“１回複製可能”の状態にある場合は、電子透かし情報を“Ｓｃｒａｍｂｌｅ（ＲＡＭ）”状態に書き換え（ステップＳ１０７）、特定のスクランブル方式に従ったスクランブル処理を実施する（ステップＳ１０８）。記録装置１０２（図３）は、このようにして生成し情報をＲＡＭディスクに記録する（ステップＳ１０９）。

【００５３】“１回複製可能”ではない場合（何度でも“複製可能”の場合）は、スクランブル処理を行わずＲＡＭディスクに記録する（ステップＳ１０９）。

【００５４】以上のようなコンプライアント記録装置１０２によって記録されたＲＡＭディスクは、複製制御が必要な“１回複製可能”な情報信号に対して、電子透かし情報としてのスクランブル情報と情報信号に対するスクランブルが対となって記録される。

【００５５】さらに、読み出し部２１３（図２）が読み出した所定の情報に基づいて、ディスク種別判別部２１４が装填されたディスクの種別を判別し、電子透かし情報にディスク種別を記録してもよい。ディスク種別は、ＲＯＭディスク（再生専用）であるか、ＲＡＭディスク（書込可能）であるか、さらには、１回書き込みのみ可能なディスクであるか、１０００回程度書き込み可能なディスクか、１０万回程度書き込み可能なディスクであるか等である。ディスクの判別は、例えば、ディスクの物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域の情報等に基づいて行われる。

【００５６】なお、スクランブル処理に関しては、情報再生時の負荷を考慮し、一部の情報のみ（ＭＰＥＧ圧縮データのＩフレームデータなど）をスクランブル対象としてもよい。この場合、電子透かし情報は、当該一部の情報全てに重畳する必要が生じる。

【００５７】なお、上記のような情報信号をスクランブルしたＲＯＭディスクを制作するような場合には、例えば、情報記録装置がオーサリングシステムとディスクカッティングシステムとして構成される。オーサリングシステムは、情報信号に応じて情報信号の圧縮処理を行うとともに、電子透かし情報としてスクランブル情報を重畳する。ディスクカッティングシステムは、情報信号に応じてスクランブル処理を施し、ディスク原盤を作成する。これらを用いれば、上述したような複製制御が可能なＲＯＭディスクを制作できる。

【００５８】［再生装置］次に図５を参照して、コンプライアント再生装置１０５の構成を説明する。なおコンプライアント再生装置１０５とコンプライアント再生装置１０１とは同じ構成である。図５は、コンプライアント再生装置１０５の構成を示すブロック図である。再生装置１０５に装填されたディスクに記録されている情報は、読み出し部４０１で読み出され、デスクランブル部４０２、スクランブル状態検出部４０３、ディスク種別判別部４０４に供給される。

【００５９】スクランブル状態検出部４０３は、付加情報としてディスクに記録されているスクランブルフラグを抽出して、記録情報にスクランブルがかかっているか否かを検出し、その検出結果をコントロール部４０５に出力する。なお、複製禁止のＲＯＭディスクには、特定暗号方式（例えば、ＣＳＳ：Ｃｏｎｔｅｎｔｓ　Ｓｃｒａｍｂｌｅ　Ｓｙｓｔｅｍ方式など）の暗号がかけられているものとする。

【００６０】ディスク種別判別部４０４は、装填されたディスクの種別を判別し、その判別結果をコントロール部４０５に供給する。ディスク種別は、ＲＯＭディスク（再生専用）であるか、ＲＡＭディスク（書込可能）であるか、さらには、１回書き込みのみ可能なディスクであるか、１０００回程度書き込み可能なディスクか、１０万回程度書き込み可能なディスクであるか等である。ディスクの判別は、例えば、ディスクの物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域の情報等に基づいて行われる。

【００６１】デスクランブル部４０２は、ＲＯＭディスクの場合には製造元で施されたスクランブルを、ＲＡＭディスクの場合には記録装置のスクランブル部２４０

（図２の（ｂ））で施されたスクランブルを解読する。デスクランブル部４０２は、図２の（ａ）を参照して説明したデスクランブル部２２０の処理を行う。

【００６２】デスクランブル部４０２は、WMデコード部４０６と再生制御部４０７に出力したデータを供給する。WMデコード部４０６は、電子透かし情報として情報信号に重畳されているスクランブル情報を復号化する。「復号化」とは、スクランブル情報を抽出し、その内容を判別することを表す。これは、電子透かし情報は雑音として情報信号に重畳されており、符号化されていると考えられるからである。WMデコード部４０６は、判別結果をコントロール部４０５に出力する。

【００６３】コントロール部４０５は、これらのディスク種別の判別結果、スクランブルフラグ、および電子透かし情報の判別出力に基づいて、再生を許可するか、禁止するかを決定する。コンプライアント記録装置１０２（図１）が記録したディスクでは、情報信号に対するスクランブルとスクランブル情報が表す内容とが対になるように記録されている。

【００６４】よってこれに違反するようなディスクが装填された場合には、デスクランブル部４０２は、再生禁止の制御情報を再生制御部４０７に供給して、この再生制御部４０７以降の処理を禁止する。正規のディスクからの情報信号の場合には、再生制御部４０７以降の処理が有効となる。再生制御部４０７は映像音声情報をデコード部４０８に供給し、デコード部４０８はＭＰＥＧ圧縮されていたデータを伸長（デコード）する。アナログＩ／Ｆ４０９は、伸長（復号）されたデータをＤ／Ａ変換し、外部の機器に供給する。また、デジタルＩ／Ｆ４１１に接続される機器がある場合には暗号化部４１０はＭＰＥＧ圧縮されたデータを暗号化し、デジタルＩ／Ｆ４１１から出力する。

【００６５】次に図６を参照して、コンプライアント再生装置１０５（図５）の再生処理を説明する。図６は、再生処理フローを示すフローチャートである。再生装置１０５（図５）では、まず装填されたディスクに記録されている情報信号に、スクランブルがかかっているか否かを判別する（ステップＳ２０１）。スクランブルには、記録装置１０２のスクランブル部２４０（図２）でかけられるＲＡＭディスク用のスクランブル方式のものと、ＲＯＭディスク用のスクランブル（例えば、ＣＳＳ方式）がある。ディスクの種別に応じてスクランブルの方式も異なるため、ディスク種別判別部４０４（図５）はディスク種別をチェックする（ステップＳ２０２）。

【００６６】ディスク種別のチェックの結果、ディスクがＲＯＭディスクである場合、デスクランブル処理部４０２（図５）はＲＯＭ用のデスクランブル処理を行う（ステップＳ２０３）。次にWMデコード部４０６（図５）は、デスクランブルされた情報信号にスクランブル状態を示す電子透かし情報（ＷＭ）が記述されているか否かをチェックし（ステップＳ２０４）、コントロール部４０５（図５）は、電子透かし情報が“Ｓｃｒａｍｂｌｅｄ（ＲＯＭ）”の状態であるかどうかを判別する（ステップＳ２０５）。“Ｓｃｒａｍｂｌｅｄ（ＲＯＭ）”の状態であるときには、コントロール部４０５（図５）は再生を許可し（ステップＳ２１１）、その状態にない時には再生を禁止する（ステップＳ２１２）。

【００６７】ステップＳ２０２におけるディスク種別のチェックの結果、ディスクがＲＡＭディスクである場合も同様に、デスクランブル処理部４０２（図５）はＲＡＭ用のデスクランブル処理を行う（ステップＳ２０６）。そしてWMデコード部４０６（図５）は、スクランブル状態を示す電子透かし情報（ＷＭ）をデスクランブルされた情報信号から検出し（ステップＳ２０７）、コントロール部４０５（図５）は、電子透かし情報が“Ｓｃｒａｍｂｌｅｄ（ＲＡＭ）”の状態であるかどうかを判別する（ステップＳ２０８）。“Ｓｃｒａｍｂｌｅｄ（ＲＡＭ）”の状態であるときには、コントロール部４０５（図５）は再生を許可し（ステップＳ２１１）、その状態にない時には再生を禁止する（ステップＳ２１２）。

【００６８】また、ステップＳ２０１でスクランブルがかかっていないと判断された場合には、デスクランブル部４０２（図５）はデスクランブル処理を行うことなく、信号情報をWMデコード部４０６（図５）に送信する。WMデコード部４０６（図５）は、電子透かし情報（ＷＭ）を検出し（ステップＳ２０９）、コントロール部４０５（図５）は電子透かし情報が“Ｓｃｒａｍｂｌｅｄ”の状態であるかどうかを判別する（ステップＳ２１０）。“Ｓｃｒａｍｂｌｅｄ”の状態にあるときは、コントロール部４０５（図５）は再生を禁止（ステップＳ２１２）し、その状態でないときは、再生を許可（ステップＳ２１１）する。ここでいう「その状態でないとき」とは、電子透かし情報が検出されないとき、または、検出された電子透かし情報が“Ｎｏｎ－Ｓｃｒａｍｂｌｅｄ”のときである。

【００６９】すなわち、コンプライアント記録装置１０２（図１）で記録されたディスクであれば、電子透かし情報WMが“Ｓｃｒａｍｂｌｅｄ”と記録されている情報信号には、スクランブル処理が行われている。しかし、電子透かし情報WMに“Ｓｃｒａｍｂｌｅｄ”と記録されているにもかかわらず情報信号がスクランブルされていないということは、その情報信号は不正に複製されたことを意味する。例えば、コンプライアント再生装置１０１（図１）の出力がノンコンプライアント記録装置１０３（図１）によりディスクに記録された場合、または、情報信号に施されているスクランブルを不正にデスクランブルし、ディスクに記録した場合が該当する。

【００７０】一方、上記のような本発明による記録装置１０２（図１、図３）ならびに再生装置１０１、１０５

（図１、図５）を用いれば、このような場合の再生を禁止することができる。これにより、再生装置に電子透かし情報を書き換えるための書換手段を実装しなくとも、不正な複製の防止が可能であり、再生装置のコストダウンが容易となる。

【００７１】なお、一部の情報信号のみがスクランブルされているような場合には、情報信号のスクランブルフラグのみではなく、デスクランブル部４０２においてデスクランブル処理が正常に行われたかどうかをチェックすることが必要である。これにより、不正に複製した情報信号のスクランブルフラグをスクランブル状態に書き換えるといった不正に対しても、再生を禁止することが可能となる。ここでは、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果が得ることができる。

【００７２】なお、実施の形態１では、光ディスクを情報記録媒体として用いた場合について説明したが、他の半導体メモリや磁気記録媒体（ハードディスクなど）についても同様である。

【００７３】（実施の形態２）実施の形態１では、記録装置１０２（図１、図３）および再生装置１０１、１０５（図１、図５）は、ディスクへの情報信号の記録、または、ディスクからの情報信号の再生を行うブロック（書き込み部３１１（図３）、読み出し部４０１（図５））、電子透かし情報を検出するブロック（WMデコード部３０７（図３）、４０６（図５））、情報信号を伸長／圧縮するブロック（エンコード部３０４（図３）、デコード部４０８（図５））とを、装置内部にすべて含むよう構成されているとして説明した。

【００７４】ところが、ＰＣで記録装置や再生装置の機能を実現する場合には、情報信号の記録・読み出しを行うドライブ部と、エンコーダ／デコーダ部とがそれぞれ別個の装置として構成されるのが一般的である。

【００７５】別個の装置として構成した場合、ドライブ部で検出したディスク種別に基づいてデコーダ部が再生制御を行うため、ディスク種別が不正にすり替えられ不正に複製したディスクが再生可能となってしまう。具体的に説明すると、ＲＯＭディスクに記録された情報信号をノンコンプライアント記録装置によりＲＡＭディスクに記録し、その後再生する場合には、ドライブ部とデコーダ部の間で不正なソフトウェアが介在することで、ドライブの検出したディスク種別を“ＲＯＭ”とすりかえることが可能である。この結果、ＲＯＭディスクをＲＡＭディスクへ不正複製した場合にコンプライアント再生装置１０１、１０５（図１）のように再生を防止できなくなる。本実施の形態は、このような場合でも再生を防止する構成を説明する。

【００７６】［ＰＣによる記録装置］図７は、パーソナルコンピュータ（ＰＣ）記録システム６００によりコンプライアント記録装置を実現した例を示す図である。図７に示すように、このようなコンプライアントなＰＣ記録システム６００は、主にＰＣエンコーダ６００－１とＰＣ記録装置（ドライブ）６００－２とから構成されており、それらの間は、不正な複製を防止可能なデジタルＩ／Ｆ（ＳＣＳＩやＡＴＡＰＩ，ＩＥＥＥ１３９４等）で接続されている。ＰＣエンコーダ６００－１は、コンプライアント記録装置１０２（図３）のＩ／Ｆ３０１、３０２（図３）からスクランブル部３１０（図３）までの構成に相当し、その動作と同じ動作を行う。したがって共通の動作に関する説明は省略する。一方、ＰＣ記録装置（ドライブ）６００－２は、書き込み部３１１（図３）の構成に相当する。

【００７７】以下、ＰＣエンコーダ６００－１の動作が、コンプライアント記録装置１０２（図３）のＩ／Ｆ３０１、３０２（図３）からスクランブル部３１０（図３）までの構成により実現される動作と異なる点を説明する。１回複製可能な情報信号をＲＡＭディスクに記録する場合には、ＰＣエンコーダ６００－１のスクランブル部６１０は、その情報信号に特定のスクランブルを施す。この際、スクランブルの基となる鍵情報をＰＣ記録ドライブとＰＣエンコーダ間で安全に共有するために、デジタルＩ／Ｆ６１５，６１６を介して認証部６１３、６１７が相互認証を行う。認証が成立した場合には、認証部６１３とＰＣ記録ドライブ中の認証部６１７との間でお互いが正規のライセンスを受けた装置、すなわちコンプライアントな装置であることを確認できる。認証が成立した場合は、さらにデジタルＩ／Ｆ上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、ＰＣエンコーダでは、暗号化部６１４において保護が必要なデータ（鍵情報や情報信号など）を暗号化し、デジタルＩ／Ｆ６１５を介して暗号化されたデータをＰＣ記録ドライブ６００－２に送信する。

【００７８】ＰＣ記録ドライブ６００－２の暗号解読部６１８は、共有化したバス鍵に基づいて受信したデータを復号する。書き込み部６１１は、ＰＣエンコーダ６００－１から受信した情報信号をＲＡＭディスク６１２に記録する。このとき記録制御部６１９は、ＰＣエンコーダに対する認証が成立していない限り、鍵情報等の特定の保護領域に記録する必要があるデータをＲＡＭディスク６１２に書き込まないよう記録制御する。

【００７９】コンプライアントな装置では、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法を変化させている。ＰＣドライブ６００－２のディスク種別判別部６２１は、読み出し部６２０から再生された信号に基づいて、ディスク６１２の物理特性（フォーカス特性、トラッキング特性、再生特性）や、ディスク６１２のコントロール領域に記録されたディスク種別を判別する。判別結果は、コントロール部６２２に出力される。なお、デ

ィスク種別を表す情報が転送中に改竄される可能性がある。しかし後述の手法によれば、そのような転送中の改竄を防止できる。コントロール部６２２では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、ＰＣエンコーダ６００－１とデータ伝送を行う。

【００８０】次に、ＰＣ記録システム６００のＰＣエンコーダ６００－１およびＰＣドライブ６００－２の処理の流れを説明する。図８は、ＰＣエンコーダ６００－１のコントロール部６０９（図７）における処理フローを示すフローチャートである。まず、１回複製可能な情報信号を記録する場合、コントロール部６０９（図７）は、認証部６１３とＰＣドライブ６００－２の認証部６１７（図７）との間で相互に認証を行わせる（ステップＳ３０１）。認証部６１３（図７）による認証の結果、コントロール部６０９（図７）は、双方がコンプライアント装置であるか否かを判別する（ステップＳ３０２）。これにより、情報信号の記録に先立って正規にライセンスを受けた機器であるか否かを確認できる。

【００８１】認証が成立した場合は、ＰＣエンコーダ６００－１とＰＣドライブ６００－２（図７）との間で共通のバス鍵を生成する（ステップＳ３０３）。そしてＰＣエンコーダ６００－１（図７）は、ＰＣドライブ６００－２（図７）で生成されたスクランブルに用いる鍵情報（以下、「スクランブル鍵情報」と称する）をＰＣドライブ６００－２から取得する（ステップＳ３０４）。スクランブル鍵情報は、共有したバス鍵に基づいてＰＣドライブ６００－２が暗号化および／または改竄防止処理を施し転送した情報である。

【００８２】ＰＣエンコーダ６００－１のコントロール部６０９（図７）では、図４と同様の記録フローにしたがって情報信号の記録を行う（ステップＳ３０５以降のステップ）。この記録フローは図４を参照して既に説明したので、その説明は省略する。

【００８３】図４のフローとの相違点は、ステップＳ１０６（図４）の“１回複製可能”の判別後に、相互認証が成立しているか否かのチェックを行うステップＳ３１１が挿入されていることである。ステップＳ３１１において相互認証が成立していない場合は、記録禁止とされる。

【００８４】続いてＰＣドライブ６００－２（図７）の処理を説明する。図９は、ＰＣ記録ドライブ６００－２のコントロール部６２２（図７）における処理フローを示すフローチャートである。先のＰＣエンコーダ６００－１と同様、１回複製可能な情報信号を記録する場合、コントロール部６２２（図７）は認証部６１７（図７）とＰＣエンコーダ６００－１の認証部６１３（図７）との間で相互に認証を行わせる（ステップＳ４０１）。そして認証部６１７（図７）による認証の結果、コントロール部６２２（図７）は、相互認証が成立したか否かを判別する（ステップＳ４０２）。

【００８５】認証が成立した場合は、コントロール部６２２（図７）は共通なバス鍵を生成する。そしてコントロール部６２２（図７）は、共有したバス鍵に基づいてスクランブル鍵情報に暗号化および／または改竄防止処理を施し、ＰＣ記録ドライブ６００－２（図７）からＰＣエンコーダ６００－１（図７）に転送を行う（Ｓ４０４）。そして、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等へのアクセス（記録や再生）を許可し、記録が行われる（ステップＳ４０５）。一方、ステップＳ４０２において相互認証が成立しない場合は、情報信号のみの記録を許可し、ディスクの一部の特定領域へのスクランブル鍵情報、スクランブル制御情報等の記録を禁止する。（ステップＳ４０６）。

【００８６】したがって、コンプライアントなＰＣエンコーダ６００－１およびＰＣドライブ６００－２（図７）同士でない場合には、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止できる。この結果、複製制御が必要な１回複製可能な情報信号の記録において、双方がコンプライアントなＰＣエンコーダ６００－１とＰＣドライブ６００－２とを組み合わせたコンプライアントＰＣシステム６００（図７）では、電子透かし情報“Ｓｃｒａｍｂｌｅｄ”と情報信号に対するスクランブル状態とが検出され、複製が可能となる。一方、ＰＣエンコーダとＰＣドライブのいずれかがノンコンプライアントなＰＣシステムでは、ディスク上の特定領域へのアクセスができず、正しいスクランブルの実施ができない。

［ＰＣによる再生装置］図１０は、パーソナルコンピュータ（ＰＣ）再生システム９００によりコンプライアント再生装置を実現した例を示す図である。図１０に示すように、このようなコンプライアントなＰＣ再生システム９００は、主にＰＣデコーダ９００－１とＰＣ再生装置（ドライブ装置）９００－２とから構成されており、それらの間は、不正な複製を防止可能なデジタルＩ／Ｆ（ＳＣＳＩやＡＴＡＰＩ，ＩＥＥＥ１３９４等）で接続されている。ＰＣデコーダ９００－１は、コンプライアント再生装置１０１、１０５（図５）のデスクランブル部４０２（図５）からＩ／Ｆ４０９、４１１（図５）までの構成に相当し、その動作と同じ動作を行う。したがって共通の動作に関する説明は省略する。一方、ＰＣ再生装置（ドライブ）９００－２は、読み出し部４０１（図５）の構成に相当する。読み出し部９０１は、このＰＣ再生装置（ドライブ）９００－２に装填されたディスク９５０から、記録されている情報を読み出し、スクランブル状態検出部９０４、ディスク種別判別部９０３に供給する。スクランブル状態検出部９０４、ディスク種別判別部９０３は、コンプライアント再生装置１０１、１０５（図５）の場合と同様に、スクランブルフラグおよびディスク種別を得る。

【００８７】ＰＣ再生装置（ドライブ）９００－２の認証部９１５は、スクランブルが施されている情報信号をデジタルＩ／Ｆ９１６から出力する場合、ＰＣデコーダ９００－１の認証部９１９との間で相互認証を行う。認証が成立していない場合には、再生制御部９１３がＰＣ再生ドライブからの情報信号の読み出しを禁止する。認証が成立した場合には、ＰＣデコーダ中のデスクランブル部９０２は、情報信号を読み出し、スクランブルが施された複製禁止の情報信号に特定のデスクランブル処理を施す。

【００８８】この際、スクランブルの基となる鍵情報をＰＣ再生ドライブとＰＣデコーダ間で安全に共有するために、デジタルＩ／Ｆ９１６、９１７を介して認証部９１５、９１９が相互認証を行う。認証が成立した場合には、認証部９１５と認証部９１９との間でお互いが正規のライセンスを受けた装置であることを確認できる。具体的には、正常に認証が成立した場合は、さらにデジタルＩ／Ｆ上に伝送するデータを暗号化するためのバス鍵を共有する。このようにして、共有化されたバス鍵を用いて、ＰＣ再生装置（ドライブ）９００－２では、暗号化部９１４において保護が必要なデータ（鍵情報や情報信号など）を暗号化し、デジタルＩ／Ｆ９１６を介して暗号化されたデータをＰＣデコーダ９００－１に送信する。

【００８９】コンプライアントな装置では、ディスク種別や記録されている情報信号によって、相互認証の方式や鍵情報と情報信号に対する処理方法を変化させている。ディスク種別判別部９０３は、読み出し部９０１の再生信号に基づいて物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域などから判別を判別する。判別結果は、コントロール部９１２に出力される。コントロール部９１２では、ディスク種別にあわせて認証方式、データの伝送方式などを切り替え、ＰＣデコーダ９００－１とのデータ伝送を行う。ＰＣデコーダ９００－１でも同様に、再生する情報信号が記録されたディスク種別や情報信号のスクランブル方式に合わせて認証方式、データの伝送方式などを切り替える。

【００９０】ＰＣデコーダ９００－１の暗号解読部９１８は、共有化したバス鍵に基づいて受信したデータを復号する。デスクランブル部９０２からＩ／Ｆ部９０９、９１１までの処理は、コンプライアント再生装置１０１、１０５（図５）の場合と同様であるのでその説明は省略する。

【００９１】ＰＣデコーダ９００－１のコントロール部９０５は、情報信号のスクランブル（スクランブルの有無やスクランブル方式）、電子透かし情報としてのスクランブル情報による再生制御のみではなく、認証方式やデータ伝送方式等も利用して再生制御を行う。

【００９２】次に、ＰＣ記録システム９００のＰＣデコーダ９００－１およびＰＣ再生装置（ドライブ）９００－２の処理の流れを説明する。図１１は、ＰＣドライブ９００－２のコントロール部９１２（図１０）における処理フローを示すフローチャートである。まず、ディスク上にスクランブルされて記録されている情報信号を再生する場合、コントロール部９１２（図１０）は、認証部９１５と、ＰＣエンコーダ６００－１の認証部９１９との間で相互に認証をを行わせる（ステップＳ５０１）。認証部９１５による認証の結果、コントロール部９１２（図１０）は、双方がコンプライアント装置であるか否かを判別する（ステップＳ５０２）。これにより、情報信号の記録に先立って正規にライセンスを受けた機器であるか否かを確認できる。

【００９３】認証が成立した場合は、ＰＣデコーダ９００－１とＰＣドライブ９００－２（図１０）との間で共通のバス鍵を生成する（ステップＳ５０３）。そしてコントロール部９１２（図１０）は、共有したバス鍵に基づいてスクランブル鍵情報に暗号化および／または改竄防止処理を施し、ＰＣドライブ９００－２（図１０）からＰＣデコーダ９００－１（図１０）に転送を行う（Ｓ５０４）。そして、スクランブルされた情報信号、ならびにスクランブル鍵情報やスクランブル制御情報等へのアクセスを許可し、再生が行われる（ステップＳ５０５）。一方、ステップＳ５０２において相互認証が成立しない場合は、情報信号のみの再生を許可し、ディスクの一部の特定領域の情報の再生を禁止する。（ステップＳ５０６）。

【００９４】図１２は、ＰＣデコーダ９００－１のコントロール部９０５（図１０）の処理フローを示すフローチャートである。先のＰＣドライブ９００－２と同様、ディスク上にスクランブルされて記録されている情報信号を再生する場合、コントロール部９０５（図１０）は、認証部９１９、認証部９１５との間で相互に認証を行わせる（ステップＳ６０１）。そして認証部９１９による認証の結果、コントロール部９０５（図１０）は、相互認証が成立したか否かを判別する（ステップＳ５０２）。

【００９５】認証が成立した場合は、ＰＣデコーダ９００－１とＰＣドライブ９００－２（図１０）との間で共通のバス鍵を生成する（ステップＳ６０３）。そしてＰＣデコーダ９００－１（図１０）は、ＰＣドライブ９００－２（図１０）で生成されたスクランブル鍵情報をＰＣドライブ９００－２から取得する（ステップＳ６０４）。

【００９６】ＰＣデコーダ９００－１のコントロール部９０５（図１０）では、図６と同様に示した再生フローにしたがって情報信号の再生を行う（ステップＳ６０５以降のステップ）。この再生フローは図６を参照して既に説明したので、その説明は省略する。

【００９７】図６のフローとの相違点は、ステップＳ２

０２（図６）のディスク種別の判別後に、それぞれのディスクに対応した相互認証が成立しているか否かのチェックを行うように変更されていることである（ステップＳ６０９、Ｓ６１２）。ＲＯＭまたはＲＡＭ用の相互認証が成立していない場合は、このような情報信号の再生禁止とされる。

【００９８】したがって、コンプライアントなＰＣデコーダ９００－１およびＰＣドライブ９００－２（図１０）同士でない場合には、スクランブル鍵情報やスクランブル制御情報等へのアクセスが防止できる。この結果、複製制御が必要な複製不可能な情報信号の再生において、双方がコンプライアントなＰＣデコーダ９００－１およびＰＣドライブ９００－２（図１０）とを組み合わせたＰＣ再生システム９００（図１０）では、情報信号に対するデスクランブル状態と電子透かし情報“Ｓｃｒａｍｂｌｅｄ”とが検出される。ノンコンプライアントＰＣシステムではディスク上の特定領域からの鍵情報の再生ができず、正規のデスクランブルを防止できる。

【００９９】［ディスク種別転送方式］次に図１３を参照して、ディスク種別を改竄されることなくＰＣドライブ部からエンコーダやデコーダに転送する方法を詳細に説明する。図１３は、ディスク種別の情報を転送する際のデータの流れを示す図である。ＰＣドライブ部は、ＰＣドライブ６００－２（図７）またはＰＣドライブ９００－２（図１０）である。

【０１００】ＰＣエンコーダまたはＰＣデコーダでは、ディスク種別を利用して情報信号の記録再生を許可する。このため、ディスク種別を表す情報を、ドライブ部からエンコーダ部またはデコーダ部に改竄されることなく転送することが必要である。ＰＣエンコーダまたはＰＣデコーダは、例えば、ＰＣエンコーダ６００－１（図７）またはＰＣデコーダ９００－１（図１０）である。

【０１０１】図１３のディスク１２５０には、ドライブ部とエンコーダ／デコーダ間の相互認証に使用する認証鍵情報１２０１が記録されている。認証鍵情報１２０１は、１または複数の暗号化認証鍵（ＥＡＫ１、ＥＡＫ２、・・・）の集合である。暗号化認証鍵は、相互認証に使用する共通鍵（認証鍵）と認証鍵情報が記録されるディスクの種別とが、デバイス鍵で暗号化された鍵である。デバイス鍵は、個々の装置に割り当てられた鍵である。

【０１０２】暗号化認証鍵の例を以下に示す。

【０１０３】ＥＡＫ１＝ＥＮＣ（デバイス鍵（ＤＫ１），｛認証鍵（ＡＫ）、ディスク種別（ＤＴ）｝）
ＥＡＫ２＝ＥＮＣ（デバイス鍵（ＤＫ２），｛認証鍵（ＡＫ）、ディスク種別（ＤＴ）｝）

ＰＣドライブの認証部９１５は、ディスク１２５０から読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵（ＥＡＫ１）を取り出し、自己が保有しているデバイス鍵ＤＫ１で復号する。この結果、認証鍵と（ＡＫ）ディスク種別（ＤＴ）が得られる。ＰＣドライブは、装填されたディスクの物理特性（フォーカス特性、トラッキング特性、再生特性）やディスク種別を記録したコントロール領域等からディスク種別（ＤＴ’）を判別する。相互認証は、認証鍵（ＡＫ）とディスク種別判別部１２０２からのディスク種別（ＤＴ’）とを特定の演算（例えば、図では加算）によって得られたディスク認証鍵（ＤＡＫ’）を用いる。

【０１０４】一方、ＰＣエンコーダ／ＰＣデコーダでは、ディスク１２５０から読み出した認証鍵情報から機器に割り当てられた暗号化認証鍵（ＥＡＫ２）を取り出し、自己が保有しているデバイス鍵ＤＫ２で復号する。この結果、認証鍵と（ＡＫ）ディスク種別（ＤＴ）が得られる。相互認証には、認証鍵（ＡＫ）とディスク種別（ＤＴ）とを特定の演算（例えば、図では加算）によって得られたディスク認証鍵（ＤＡＫ）を用いる。

【０１０５】このようにして共有化したディスク認証鍵を用いて相互認証を行う。すなわち、ＤＡＫ＝ＤＡＫ’の場合は相互認証が成立し、ＤＡＫ≠ＤＡＫ’の場合は相互認証が成立しない。つまり、認証部９１５および９１９は、認証鍵情報のＤＴとドライブが検出したＤＴ’が一致しない時には、認証を不成立にできる。この結果、ＲＯＭディスクから入手した情報信号や鍵情報をＲＡＭディスクに不正に複製したとしても、認証鍵情報中のディスク種別（ＤＴ）とドライブが検出するディスク種別（ＤＴ’）とは不一致となる。よって相互認証が成立せず、情報信号の再生を防止できる。また、認証鍵情報を不正にすりかえたとしても、認証鍵やディスク種別が不一致となり、相互認証が不成立となる。

【０１０６】なお、認証鍵情報に認証鍵とディスク種別を暗号化して記録した場合を説明した。しかし、認証鍵情報にディスク種別を含めず、ドライブで検出したディスク種別を暗号化してＰＣエンコーダやデコーダに伝送し、復号してディスク種別を得る方法であっても、ディスク種別を安全に転送することができる。よって実質的に正常な情報信号の再生は可能である。認証鍵情報にディスク種別を含めない場合には相互認証がディスクの種別によらず共通になり、ディスク種別によらず相互認証は成立する。ただし相互認証は成立していても、誤ったディスク種別（スクランブル方式）で情報信号が再生される場合には映像や音声が正しく表示されなくすることもできる。

【０１０７】上記のような記録装置または再生装置によると、ＰＣドライブ部にＷＭ検出部やＷＭ書換部を実装しなくても、不正な複製ディスクの再生を防止できる。

【０１０８】次に、ディスク種別によって認証方式やデータの伝送方式（データや鍵情報の伝送手順）を変化させる処理を説明する。この性質を逆に利用すれば、認証を行った処理手順からディスク種別の判別を行う処理も可能である。以下の説明は、（図１０）ＰＣドライブと

ＰＣデコーダとして利用可能なシステムである。

【０１０９】図１４は、再生システム１４００がＤＶＤ－ＲＯＭディスク１４５０を再生する場合の認証手順とデータ転送手順を示す。まずバス認証ステップを説明する。ＭＰＥＧデコーダモジュール１４２８が乱数c1を生成し、チャレンジデータ(drv_chal(c1))としてＤＶＤドライブ１４００－１にセットする。ＤＶＤドライブ１４００－１は、秘密情報である関数fを用いてf(c1)を生成し、レスポンスデータ(drv_res(f(c1))としてＭＰＥＧデコーダモジュール１４００－２に返す。ＭＰＥＧデコーダモジュール１４００－２は、自らが有する秘密情報である関数fを用いてf(c1)を生成する。そしてＭＰＥＧデコーダモジュール１４００－２は、f(c1)がＤＶＤドライブ１４００－１から返されたレスポンスデータと一致しているかどうかをチェックし、ＭＰＥＧデコーダ１４２８はDVDドライブ１４００－１がコンプライアントな機器であることを確認する。

【０１１０】次に、ＤＶＤドライブ１４００－１が乱数c2を生成し、チャレンジデータとしてＭＰＥＧデコーダモジュール１４００－２にセットする(dec_chal(c2))。ＭＰＥＧデコーダモジュール１４００－２は、秘密情報である関数fを用いてf(c2)を生成し、レスポンスデータとしてＤＶＤドライブ１４００－１に返す(dec_res(f(c2))。ＤＶＤドライブ１４００－１は、自らが有する秘密情報である関数fを用いてf(c2)を生成する。そしてＤＶＤドライブ１４００－１は、f(c2)がＭＰＥＧデコーダモジュール１４００－２から返されたレスポンスデータと一致しているかどうかをチェックし、DVDドライブはＭＰＥＧデコーダがコンプライアントな機器であることを確認する。この結果、DVDドライブ１４００－１とＭＰＥＧデコーダモジュール１４００－２の間で秘密の時変鍵が共有される。

【０１１１】続いて時変鍵を用いた鍵情報の秘密伝送ステップを説明する。ＤＶＤドライブ１４００－１は、共有した時変鍵を用いてＤＶＤ－ＲＯＭディスク１４５０に記録された暗号化ディスク鍵セットと暗号化タイトル鍵をバス暗号化し、ＭＰＥＧデコーダモジュール１４００－２に転送する。ＭＰＥＧデコーダモジュール１４００－２では、受け取ったバス暗号化された暗号化ディスク鍵セットと暗号化タイトル鍵を、共有した時変鍵を用いてバス復号化する。

【０１１２】スクランブルされた情報信号の復号に関して、ＭＰＥＧデコーダモジュール１４００－１２は、バス復号化された暗号化ディスク鍵セットと暗号化タイトル鍵を利用して、図２の（ａ）に示すようにスクランブルされた情報信号を復号して、コンテンツとしての情報信号を得ることができる。

【０１１３】図１５は、再生システム１５００がＤＶＤ－Ｒディスク１５５０を再生する場合の認証手順とデータ転送手順を示す。まずバス認証ステップは、上述のＤＶＤ－ＲＯＭ１４５０（図１４）ディスクを再生する場合のバス認証ステップと同じである。したがってその説明は省略する。次に時変鍵を用いた鍵情報の秘密伝送ステップを説明する。ＤＶＤドライブ１５００－１は、共有した時変鍵を用いて暗号化ディスク鍵セットをバス暗号化し、メディアＩＤに改ざんチェックコードを付与する。そしてＤＶＤドライブ１５００－１は、暗号化ディスク鍵セットとメディアＩＤとをＭＰＥＧデコーダモジュール１５００－２に転送する。ＭＰＥＧデコーダモジュール１５００－２は、受け取ったバス暗号化された暗号化ディスク鍵セットを、共有した時変鍵を用いてバス復号化する。またＭＰＥＧデコーダモジュール１５００－２では、メディアＩＤに付与されている改ざんチェックコードを、共有した時変鍵を用いてチェックする。

【０１１４】最後にスクランブルされた情報信号（コンテンツ）の復号を説明する。ＭＰＥＧデコーダモジュール１５００－２は、ＤＶＤ－Ｒディスク１５５０のユーザ領域から暗号化タイトル鍵とスクランブルされた情報信号（ＡＶデータ）を読み出す。そしてＭＰＥＧデコーダモジュール１５００－２は、復号化された暗号化ディスク鍵セットでディスク鍵を復号し、そのディスク鍵でディスク固有鍵を復号する。さらにそのディスク固有鍵でタイトル鍵を復号し、そのタイトル鍵でスクランブルされた情報信号をデスクランブルする。

【０１１５】上記のように、スクランブルされた情報信号の復号に必要となる鍵等の情報は、再生型ＤＶＤ（ＤＶＤ－ＲＯＭディスク）と記録型ＤＶＤ（ＤＶＤ－Ｒディスク）とで異なるので、転送されるデータや転送手順が異なる。本発明は、ＤＶＤドライブでディスク種別を識別し、それに対応した転送手順に従うように制御する。ＭＰＥＧデコーダモジュールでは、データ転送手順の違いからディスク種別を識別し、電子透かし情報に重畳されているディスク種別と一致比較することによって、再生制限を行うことができる。なお図１４および図１５では、再生型ＤＶＤと記録型ＤＶＤとで同じ認証方法を用いている。しかし再生型ＤＶＤと記録型ＤＶＤとで異なる認証方法を用いることで、認証方法の相違からＭＰＥＧデコーダモジュールは上記の場合と同様にディスク種別を識別できる。異なる認証方法としては、異なるアルゴリズム（上記関数f）を使用する認証方法、および、同一のアルゴリズムであってもアルゴリズム中で異なるパラメータを使用するなどがある。これまでの説明では、スクランブルにより情報信号に対する暗号化を行ったが、他の方式を用いて暗号化を行った場合も同様の効果が得ることができる。

【０１１６】本実施の形態では、光ディスクを情報記録媒体として用いた場合について説明した。しかしその説明は、他の半導体メモリや磁気記録媒体（ハードディスクなど）についても同様の方法で適用可能である。また、本発明の暗号化された情報信号は、インターネット

等のネットワーク回線（伝送媒体）や、デジタル放送等の番組として電波で伝送されてもよい。このとき上述した認証手順により、受信側と送信側とで認証を行うことで、不正な複製を防止できる。

【０１１７】

【発明の効果】以上説明したように、本発明によれば、所定の複製制御の対象となる情報信号（例えば、これ以上複製禁止、または、絶対複製禁止の情報信号）に対しては、当該情報信号がスクランブルされていることを示すスクランブル情報を電子透かし情報として重畳し、かつ、情報記録媒体の種別にしたがったスクランブルを行って情報記録媒体への記録を行うようにした。これにより、スクランブルを解読した後の情報記録媒体への不正な記録や、不正に複製した他の種類の情報記録媒体からの再生を制限できる。後者についてより具体的には、情報再生装置は、読み出した情報信号に重畳されている電子透かし情報（スクランブル情報）の示す状態と、読み出した情報信号のスクランブル状態（スクランブルされているか否か）を比較する。これにより、比較結果が不一致の場合には、不正な複製によって作成された情報記録媒体からの再生であるとして、その再生を防止できる。なお本発明によれば、情報再生装置において電子透かし情報の書き換えは行わないので、電子透かし情報の書換手段を実装する必要がなく、安価な構成をとることができる。

【図面の簡単な説明】

【図１】　実施の形態１による複製世代管理方法を説明するための概略図である。

【図２】　スクランブルされた信号情報の読み出しまたは書き込みを行う際のデータの流れを示す図である。

【図３】　コンプライアント記録装置の構成を示す図である。

【図４】　記録装置の記録処理フローを示すフローチャートである。

【図５】　コンプライアント再生装置の構成を示すブロック図である。

【図６】　再生処理フローを示すフローチャートである。

【図７】　パーソナルコンピュータ（ＰＣ）記録システムによりコンプライアント記録装置を実現した例を示す図である。

【図８】　ＰＣエンコーダのコントロール部における処理フローを示すフローチャートである。

＊【図９】　ＰＣ記録ドライブのコントロール部における処理フローを示すフローチャートである。

【図１０】　パーソナルコンピュータ（ＰＣ）再生システムによりコンプライアント再生装置を実現した例を示す図である。

【図１１】　ＰＣドライブのコントロール部における処理フローを示すフローチャートである。

【図１２】　ＰＣデコーダのコントロール部の処理フローを示すフローチャートである。

【図１３】　ディスク種別の情報を転送する際のデータの流れを示す図である。

【図１４】　再生システムがＤＶＤ－ＲＯＭディスクを再生する場合の認証手順とデータ転送手順を示す。

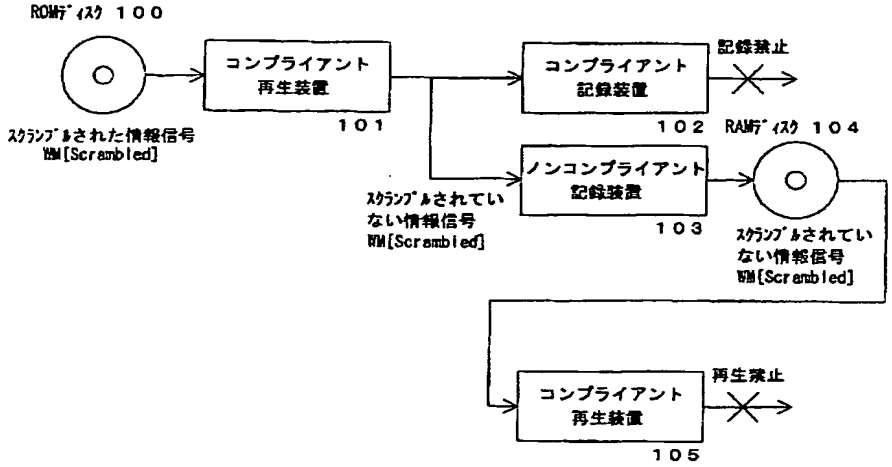
【図１５】　再生システムがＤＶＤ－Ｒディスクを再生する場合の認証手順とデータ転送手順を示す。

【図１６】　従来の複製制御の原理を示す図である。

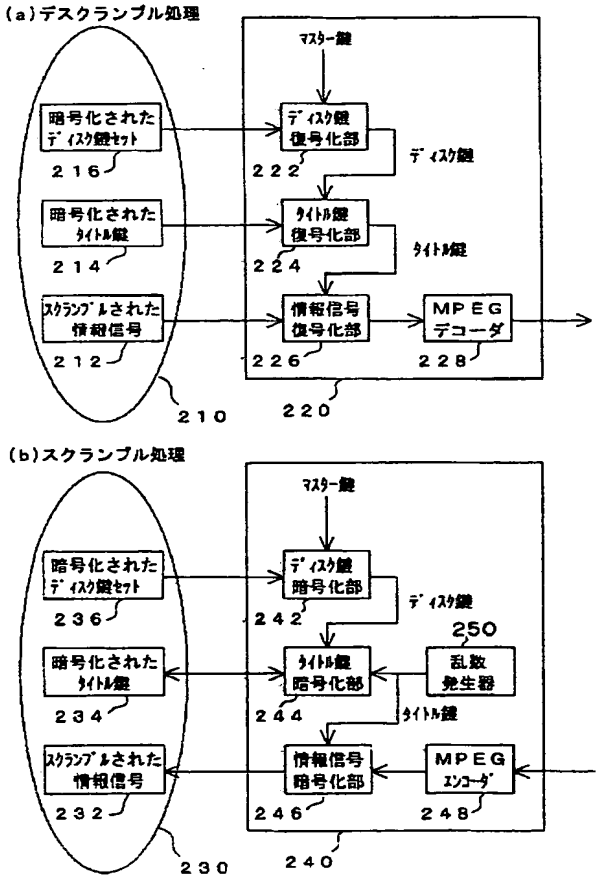
【符号の説明】

１０１　コンプライアント再生装置
１０２　コンプライアント記録装置
１０５　コンプライアント再生装置
３０１　デジタルＩ／Ｆ
３０２　アナログＩ／Ｆ
３０３　暗号解読部
３０４　エンコード部
３０６　ＷＭ書換部
３０７　ＷＭデコード部
３０８　記録制御部
３０９　コントロール部
３１０　スクランブル部
３１１　書込み部
３１３　読み出し部
３１４　ディスク種別判別部
４０１　読み出し部
４０２　デスクランブル部
４０３　スクランブル状態検出部
４０４　ディスク種別判別部
４０５　コントロール部
４０６　ＷＭデコード部
４０７　再生制御部
４０８　デコード部
４０９　アナログＩ／Ｆ
４１０　暗号化部
４１１　デジタルＩ／Ｆ

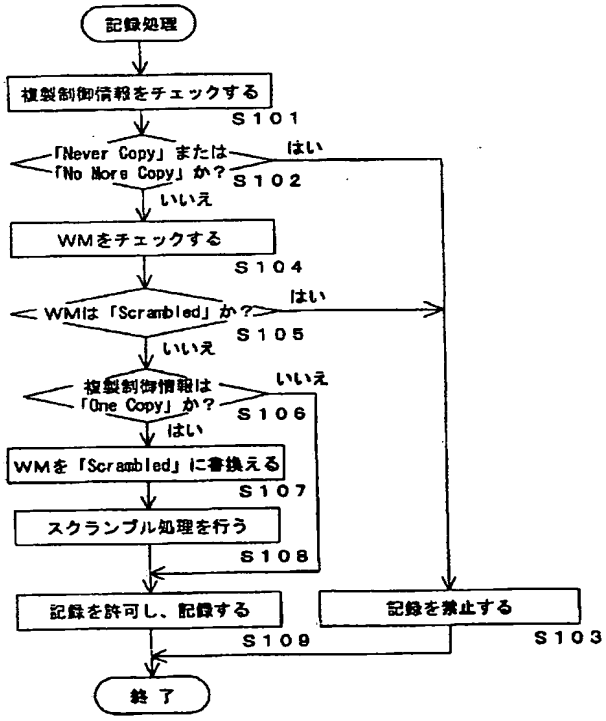
【図１】


ROMﾃﾞｨｽｸ １００
ｽｸﾗﾝﾌﾞﾙされた情報信号
WM[Scrambled]
コンプライアント
再生装置
１０１
コンプライアント
記録装置
１０２
記録禁止
RAMﾃﾞｨｽｸ １０４
ﾉﾝｺﾝﾌﾟﾗｲｱﾝﾄ
記録装置
１０３
ｽｸﾗﾝﾌﾞﾙされていない情報信号
WM[Scrambled]
ｽｸﾗﾝﾌﾞﾙされていない情報信号
WM[Scrambled]
コンプライアント
再生装置
１０５
再生禁止

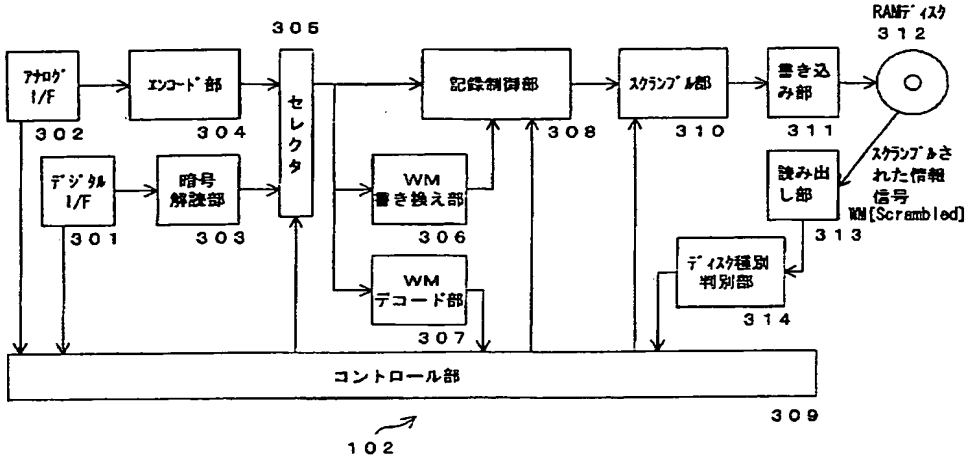
【図２】


(a)デスクランブル処理
ﾏｽﾀｰ鍵
暗号化された
ﾃﾞｨｽｸ鍵ｾｯﾄ
２１６
ﾃﾞｨｽｸ鍵
復号化部
２２２
ﾃﾞｨｽｸ鍵
暗号化された
ﾀｲﾄﾙ鍵
２１４
ﾀｲﾄﾙ鍵
復号化部
２２４
ﾀｲﾄﾙ鍵
ｽｸﾗﾝﾌﾞﾙされた
情報信号
２１２
情報信号
復号化部
２２６
MPEG
ﾃﾞｺｰﾀﾞ
２２８
２１０
２２０
(b)スクランブル処理
ﾏｽﾀｰ鍵
暗号化された
ﾃﾞｨｽｸ鍵ｾｯﾄ
２３６
ﾃﾞｨｽｸ鍵
暗号化部
２４２
ﾃﾞｨｽｸ鍵
２５０
暗号化された
ﾀｲﾄﾙ鍵
２３４
ﾀｲﾄﾙ鍵
暗号化部
２４４
乱数
発生器
ﾀｲﾄﾙ鍵
ｽｸﾗﾝﾌﾞﾙされた
情報信号
２３２
情報信号
暗号化部
２４６
MPEG
ｴﾝｺｰﾀﾞ
２４８
２３０
２４０

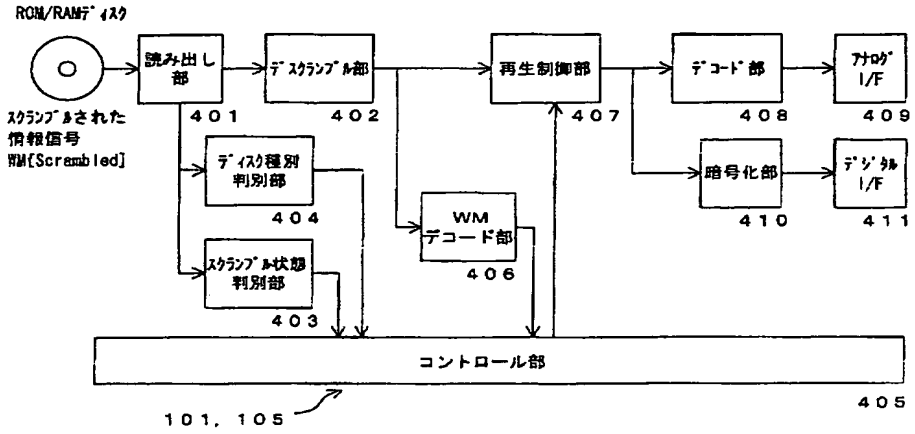
【図４】


記録処理
複製制御情報をチェックする
S１０１
「Never Copy」または
「No More Copy」か？
S１０２
はい
いいえ
WMをチェックする
S１０４
WMは「Scrambled」か？
S１０５
はい
いいえ
複製制御情報は
「One Copy」か？
S１０６
いいえ
はい
WMを「Scrambled」に書換える
S１０７
スクランブル処理を行う
S１０８
記録を許可し、記録する
S１０９
記録を禁止する
S１０３
終了

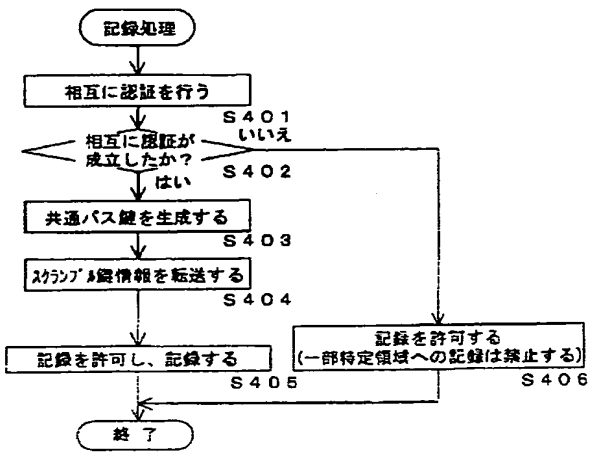
【図３】


305
RAMﾃﾞｨｽｸ
312
ｱﾅﾛｸﾞ I/F
302
ｴﾝｺｰﾄﾞ部
304
セレクタ
記録制御部
308
ｽｸﾗﾝﾌﾞﾙ部
310
書き込み部
311
ﾃﾞｼﾞﾀﾙ I/F
301
暗号解読部
303
WM 書き換え部
306
読み出し部
313
ｽｸﾗﾝﾌﾞﾙされた情報信号
WM[Scrambled]
WM デコード部
307
ﾃﾞｨｽｸ種別判別部
314
コントロール部
309
102

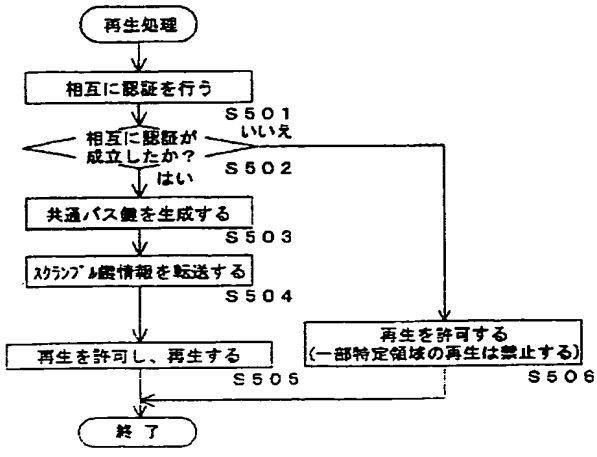
【図５】


ROM/RAMﾃﾞｨｽｸ
ｽｸﾗﾝﾌﾞﾙされた情報信号
WM[Scrambled]
読み出し部
401
ﾃﾞｽｸﾗﾝﾌﾞﾙ部
402
再生制御部
407
ﾃﾞｺｰﾄﾞ部
408
ｱﾅﾛｸﾞ I/F
409
ﾃﾞｨｽｸ種別判別部
404
WM デコード部
406
暗号化部
410
ﾃﾞｼﾞﾀﾙ I/F
411
ｽｸﾗﾝﾌﾞﾙ状態判別部
403
コントロール部
405
101, 105

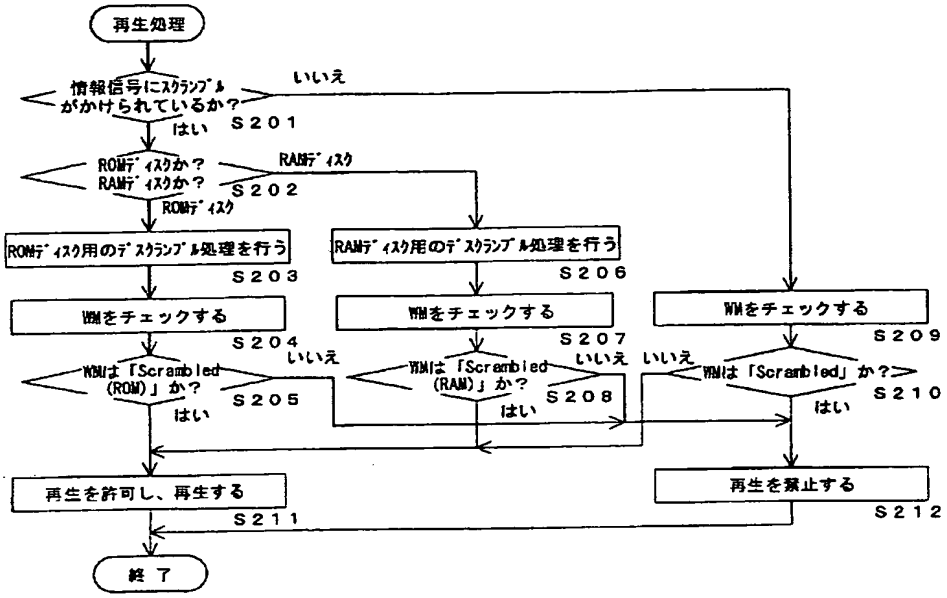
【図９】


記録処理
相互に認証を行う
S401
相互に認証が成立したか？
いいえ
はい
S402
共通パス鍵を生成する
S403
ｽｸﾗﾝﾌﾞﾙ鍵情報を転送する
S404
記録を許可し、記録する
S405
記録を許可する
(一部特定領域への記録は禁止する)
S406
終了

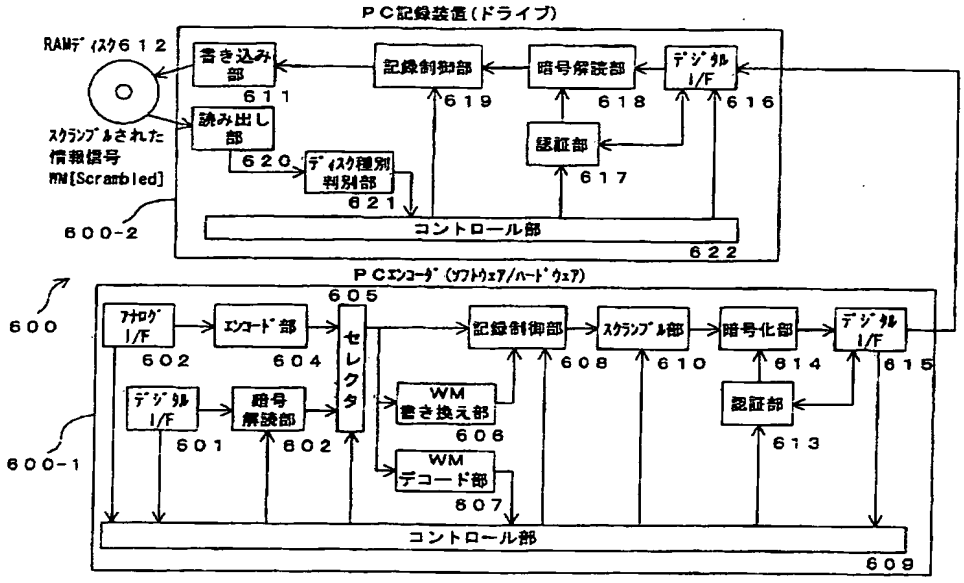
【図１１】


再生処理
相互に認証を行う
S501
相互に認証が成立したか？
いいえ
はい
S502
共通パス鍵を生成する
S503
ｽｸﾗﾝﾌﾞﾙ鍵情報を転送する
S504
再生を許可し、再生する
S505
再生を許可する
(一部特定領域の再生は禁止する)
S506
終了

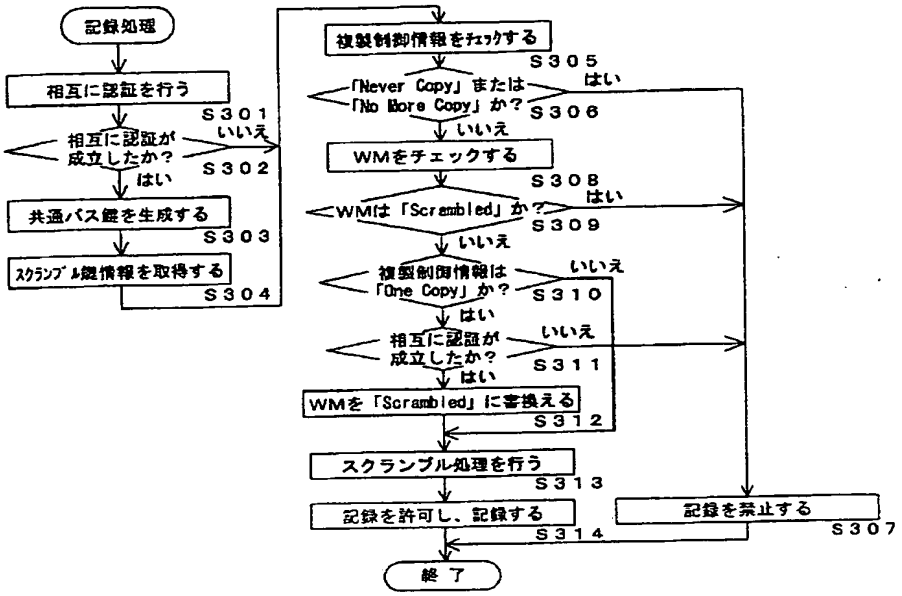
【図６】


再生処理
情報信号にｽｸﾗﾝﾌﾞﾙがかけられているか？
いいえ
はい
Ｓ２０１
ROMﾃﾞｨｽｸか？
RAMﾃﾞｨｽｸか？
RAMﾃﾞｨｽｸ
ROMﾃﾞｨｽｸ
Ｓ２０２
ROMﾃﾞｨｽｸ用のﾃﾞｽｸﾗﾝﾌﾞﾙ処理を行う
Ｓ２０３
RAMﾃﾞｨｽｸ用のﾃﾞｽｸﾗﾝﾌﾞﾙ処理を行う
Ｓ２０６
WMをチェックする
Ｓ２０４
WMをチェックする
Ｓ２０７
WMをチェックする
Ｓ２０９
WMは「Scrambled(ROM)」か？
いいえ
はい
Ｓ２０５
WMは「Scrambled(RAM)」か？
いいえ
はい
Ｓ２０８
WMは「Scrambled」か？
いいえ
はい
Ｓ２１０
再生を許可し、再生する
Ｓ２１１
再生を禁止する
Ｓ２１２
終了

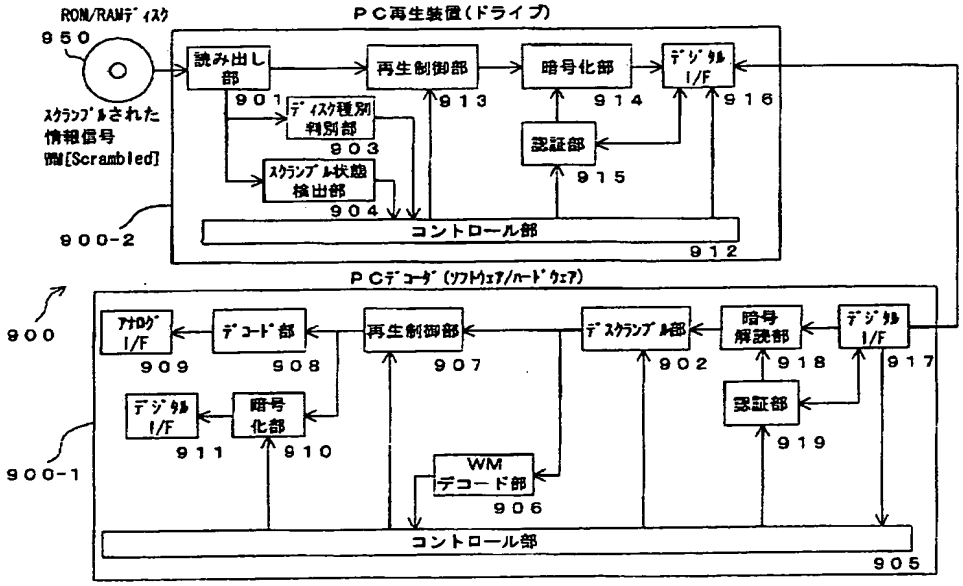
【図７】


ＰＣ記録装置（ドライブ）
RAMﾃﾞｨｽｸ６１２
ｽｸﾗﾝﾌﾞﾙされた情報信号 WM[Scrambled]
６００-２
書き込み部
６１１
読み出し部
６２０
ﾃﾞｨｽｸ種別判別部
６２１
記録制御部
６１９
暗号解読部
６１８
ﾃﾞｼﾞﾀﾙI/F
６１６
認証部
６１７
コントロール部
６２２
ＰＣｴﾝｺｰﾀﾞ（ｿﾌﾄｳｪｱ/ﾊｰﾄﾞｳｪｱ）
６００
６００-１
６０５
ｱﾅﾛｸﾞI/F
６０２
ｴﾝｺｰﾄﾞ部
６０４
ｾﾚｸﾀ
ﾃﾞｼﾞﾀﾙI/F
６０１
暗号解読部
６０３
WM書き換え部
６０６
WMﾃﾞｺｰﾄﾞ部
６０７
記録制御部
６０８
ｽｸﾗﾝﾌﾞﾙ部
６１０
暗号化部
６１４
ﾃﾞｼﾞﾀﾙI/F
６１５
認証部
６１３
コントロール部
６０９

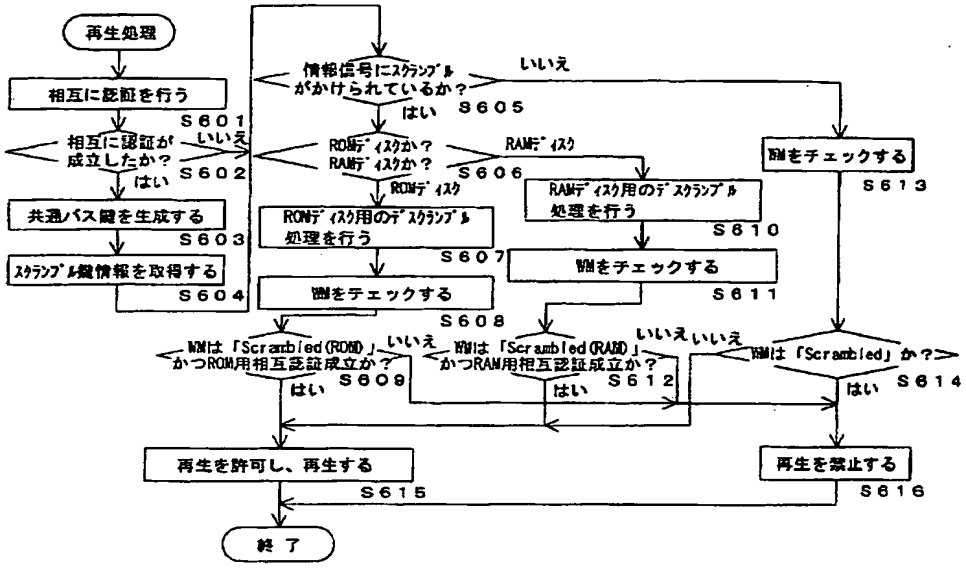
【図８】


記録処理
相互に認証を行う
S301
相互に認証が成立したか？
いいえ
S302
はい
共通バス鍵を生成する
S303
スクランブル鍵情報を取得する
S304
複製制御情報をチェックする
S305
「Never Copy」または「No More Copy」か？
はい
S306
いいえ
WMをチェックする
S308
WMは「Scrambled」か？
はい
S309
いいえ
複製制御情報は「One Copy」か？
いいえ
S310
はい
相互に認証が成立したか？
いいえ
S311
はい
WMを「Scrambled」に書換える
S312
スクランブル処理を行う
S313
記録を許可し、記録する
S314
記録を禁止する
S307
終了

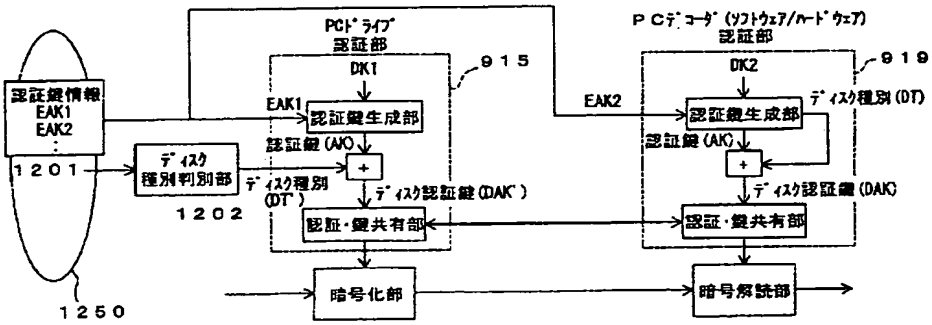
【図１０】


ROM/RAMディスク
950
スクランブルされた情報信号例[Scrambled]
900-2
PC再生装置(ドライブ)
読み出し部
901
再生制御部
913
暗号化部
914
デジタルI/F
916
ディスク種別判別部
903
スクランブル状態検出部
904
認証部
915
コントロール部
912
PCデコーダ(ソフトウェア/ハードウェア)
900
アナログI/F
909
デコード部
908
再生制御部
907
デスクランブル部
902
暗号解読部
918
デジタルI/F
917
デジタルI/F
911
暗号化部
910
900-1
認証部
919
WMデコード部
906
コントロール部
905

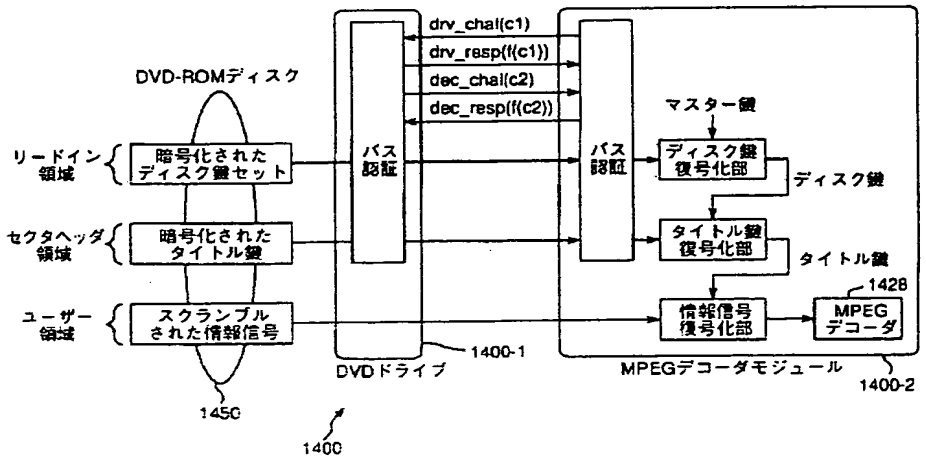
【図１２】


再生処理
相互に認証を行う
S601
相互に認証が成立したか？
いいえ
はい
S602
共通バス鍵を生成する
S603
スクランブル鍵情報を取得する
S604
情報信号にスクランブルがかけられているか？
いいえ
はい
S605
ROMディスクか？
RAMディスクか？
RAMディスク
ROMディスク
S606
RAMディスク用のデスクランブル処理を行う
S610
WMをチェックする
S611
ROMディスク用のデスクランブル処理を行う
S607
WMをチェックする
S608
WMをチェックする
S613
WMは「Scrambled(ROM)」かつROM用相互認証成立か？
いいえ
はい
S609
WMは「Scrambled(RAM)」かつRAM用相互認証成立か？
いいえ
はい
S612
WMは「Scrambled」か？
いいえ
はい
S614
再生を許可し、再生する
S615
再生を禁止する
S616
終了

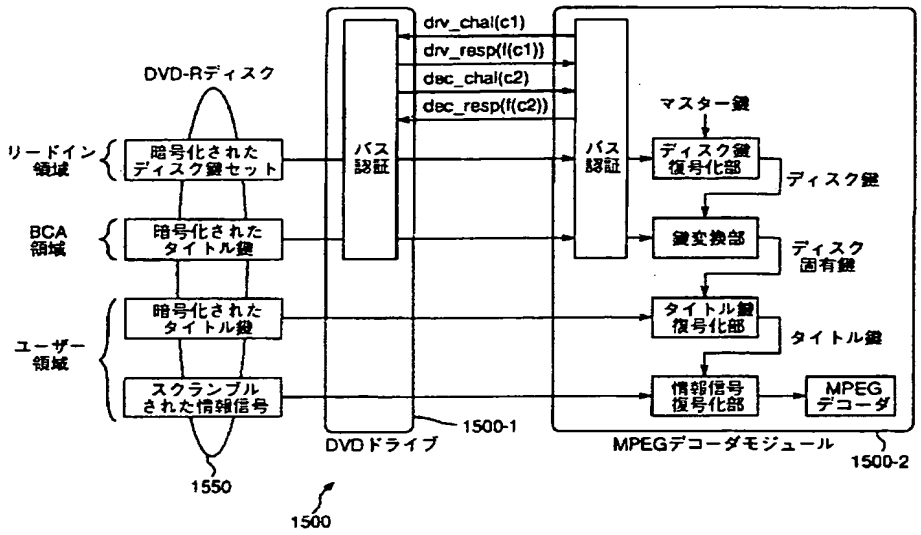
【図１３】


PCドライブ認証部
DK1
915
EAK1
認証鍵生成部
認証鍵(AK)
ディスク種別判別部
1202
ディスク種別(DT)
ディスク認証鍵(DAK)
認証・鍵共有部
暗号化部
認証鍵情報
EAK1
EAK2
1201
1250
PCデコーダ(ソフトウェア/ハードウェア)認証部
DK2
919
EAK2
認証鍵生成部
ディスク種別(DT)
認証鍵(AK)
ディスク認証鍵(DAK)
認証・鍵共有部
暗号解読部

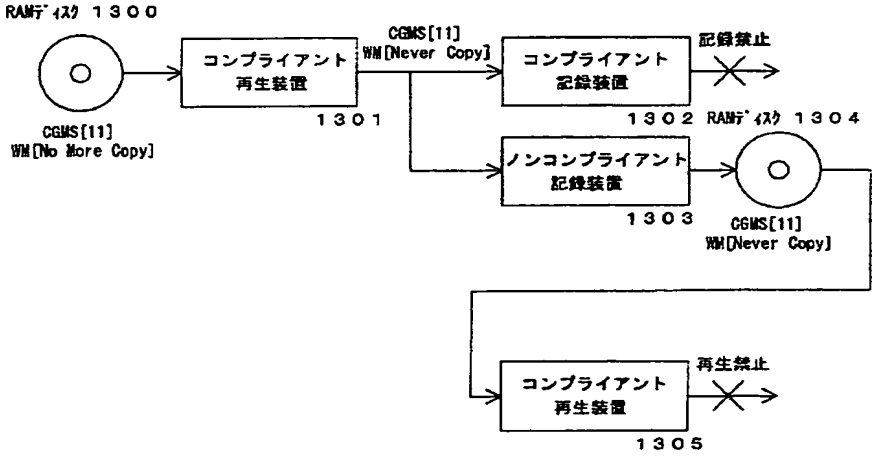
【図１４】


DVD-ROMディスク
リードイン領域
暗号化されたディスク鍵セット
セクタヘッダ領域
暗号化されたタイトル鍵
ユーザー領域
スクランブルされた情報信号
1450
1400
drv_chal(c1)
drv_resp(f(c1))
dec_chal(c2)
dec_resp(f(c2))
バス認証
DVDドライブ
1400-1
マスター鍵
ディスク鍵復号化部
ディスク鍵
タイトル鍵復号化部
タイトル鍵
情報信号復号化部
1428
MPEGデコーダ
MPEGデコーダモジュール
1400-2

【図１５】



【図１６】



フロントページの続き

(51)Int.Cl.⁷		識別記号	F I		テーマコード（参考）
H04N	1/387		H04L	9/00	601A
	1/40		H04N	1/40	Z
	5/91			5/91	P